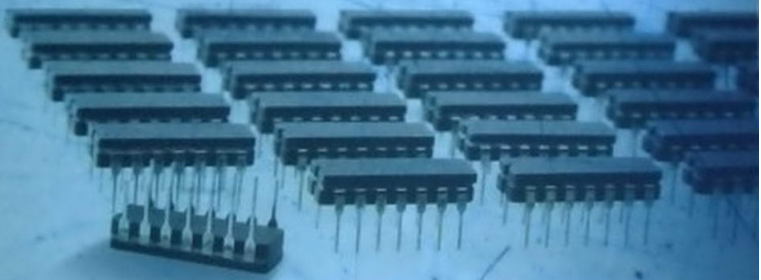
JAMES F. DUNNIGAN

NOUA AMENINȚARE MONDIALĂ

CYBER-TERORISMUL



Săptămâna Financiară

Curtea veche

JAMES F. DUNNIGAN
Noua ameninţare mondială
Cyber-terorismul

Traducere din limba engleză de NICOLETA STROIE
BUCUREŞTI, 2010

JAMES F. DUNNIGAN este analist militar şi designerul a peste 100 de jocuri pe calculator ce reproduc situaţii de război. Este recunoscut şi apreciat pentru modul realist în care analizează teatrele de război din lumea întreagă. Susţine în mod regulat cursuri de istorie militară la instituţii academice din Statele Unite şi participă des în emisiuni de televiziune în calitate de comentator al subiectelor militare.

Descrierea CIP a Bibliotecii Naţionale a României DUNNIGAN, JAMES F.
Noua ameninţare mondială: cyber-terorismul / James F. Dunnigan; trad.: Nicoleta Stroie.
— Bucureşti: Curtea Veche Publishing, 2010
ISBN 978 – 973 – 669 – 937 – 5
I. Stroie, Nicoleta (trad.) 343.23: 004
004.052
Coperta: GRIFFON AND SWANS
www.griffon. ro

JAMES F. DUNNIGAN
The Next War Zone:
Confronting the Global Threat of Cyberterrorism
2002, James F. Dunnigan
CURTEA VECHE PUBLISHING, 2009

ISBN 978 – 973 – 669 – 937.5

PREFAŢĂ LA EDIŢIA A DOUA

OK, după multă redactare, are acum 120.000 de cuvinte. Am tăiat o mulţime de lucruri, dar am adăugat şi mai multe, în special termenii din glosar.

8 aprilie 2002

Întotdeauna este complicat să scrii o carte despre tehnologie, pentru că aceasta are tendinţa de a se dezvolta într-un ritm alert. Este diferit de a scrie un articol de revistă, care ajunge la tipar câteva săptămâni mai târziu**,** cel mult câteva luni, pentru ca apoi, când apare următorul număr al publicaţiei, textul să devină istorie. Este nevoie de mai mult timp pentru a scrie o carte, pentru că aceasta presupune mai multe lucruri şi este nevoie de mai mult timp (6 – 12 luni) până ajunge la tipar odată ce manuscrisul este acceptat. După aceea, cărţile stau pe un raft şi sunt considerate

„De actualitate" până când va deveni mult prea evident că mi mai sunt aşa. Mi-am încercat norocul cu *Noua ameninţare mondială,* crezând că este posibil să realizez o abordare istorică a internetului şi să scriu o carte care să fie atât de actualitate, cât şi de durată. Şi bazându-mă pe reacţiile cititorilor, se pare că aşa s-a şi întâmplat. O mare parte din istoria internetului nu era cunoscută nici măcar pentru tocilarii autentici. Cel mai important, această abordare istorică mi-a dat posibilitatea sa îmi îndrept atenţia cu încredere asupra problemelor majore de securitate care nu aveau să sufere modificări în viitorul apropiat.

Deşi este uşor să dai vina pe Microsoft pentru toate problemele de securitate ale webului, nu este cu adevărat vina lui. Doamne, urăsc să spun asta, dar trebuie să dai dreptate şi diavolului. Dacă nu ar exista Microsoft, cineva ar trebui să îl inventeze pentru ca webul să se dezvolte

atât de mult într-un timp atât de scurt. Întrucât mă aflu în domeniul computerelor încă de la începutul anilor ’70, iar în mediul online din 79, am fost chiar în mijlocul evenimentelor când PC-urile au evoluat de la kiturile de execuţie proprie până la „fermele” de servere cu mii de PC-uri compacte (modelul *blade),* fiecare cu o putere de procesare mai mare decât un computer ultraperformant de mai multe milioane de dolari din perioada anilor ’70. Viteza şi deschiderea ce au caracterizat dezvoltarea tehnologiei PC-ului necesitau apariţia cuiva ca Microsoft, pentru ca nu cumva creşterea să fie oprită în anii ’80, când mai multe sisteme de operare se aflau în competiţie, iar producătorii de software stăteau pe margine, aşteptând să câştige cineva. În tot acest interval, utilizatorii nu erau prea dornici să cumpere PC-uri. De fapt, acest lucru s-a întâmplat în Japonia, dar nu şi în Coreea de Sud. Motiv pentru care, deşi are o economie mult mai slab dezvoltată, Coreea de Sud are o cultură a PC-ului mult mai puternică decât cea a Japoniei. Standardizarea a schimbat situaţia, dar, aşa cum este explicat în carte, a adus cu ea şi toate problemele pe care le avem în prezent legate de vulnerabilitatea internetului.

Când citeşti despre tot felul de noi atacuri pe internet şi noi metode de apărare, vezi că toate urmează acelaşi tipar. Erorile apărute în software-ul de internet sunt folosite de către hackeri pentru a pătrunde în computerele altor persoane. Acele erori sunt remediate, dar altele noi apar în permanenţă. Atunci când urmăreşti evoluţia internetului încă dinainte de începuturi (pe când aceste neplăceri erau transmise prin sistemul BBS), poţi observa ce tipare se formează. La fel ca în orice strategie de luptă de succes, trebuie să profiţi de fiecare punct slab din apărarea celorlalţi. Altfel, planul tău nu funcţionează. Asta este ceea ce s-a întâmplat şi în cazul multor metode de atac pe internet, dar, de regulă, mass-media nu fac publice toate atacurile eşuate.

Înainte ca majoritatea utilizatorilor de PC să intre în mediul online, cea mai comună modalitate a software-ului rău intenţionat de a contamina computerele era prin intermediul dischetelor care circulau printre elevi sau colecţionarii de software furat. Cele două grupuri aveau foarte multe tangenţe. Într-un scenariu tipic, puştiul venea acasă cu o dischetă plină de „chestii interesante”, pe care un prieten i le copiase pe un PC de la şcoală. Copilul introducea discheta în computerul tatălui şi îl virusa. A doua zi, tatăl copia nişte fişiere pe o altă dischetă, pe care o lua la serviciu, infectând şi PC-urile de acolo. Chiar dacă nu s-au dezvoltat cu aceeaşi viteză ca internetul, programele periculoase s-au răspândit destul de repede.

Aşa cum este explicat în carte, internetul a furnizat pur şi simplu mai multe oportunităţi pentru acest tip de înşelăciune. În vreme ce înainte descărcarea prin BBS a unui software-capcană era cel mai puţin periculos mod de a obţine aşa ceva, în ceea ce priveşte internetul, acesta a fost cea mai uşoară modalitate de a răspândi viruşi, cai troieni, viermi informatici şi tot ce vrei. Era mult mai convenabil decât dischetele, mai ales pentru că viteza modemurilor a crescut de la 300 bps, cât avea în anul 1979, la 28.000 bps atunci când a apărut internetul, la mijlocul anilor ’90, pentru ca ulterior să ajungă la 56.000 bps până la sfârşitul anilor ’90. Comoditatea are întotdeauna un preţ ascuns de plătit.

Dat fiind că am scris multe cărţi despre istoria militară şi tehnologică, am văzut tiparele vechi de secole ale înfruntării „noilor arme” de către noi „mijloace”. Asta este ceea ce se întâmplă cu internetul, iar tu le afli în mijlocul confruntării pentru că îl accesezi.

Citeşte această carte şi îţi voi arăta cum îţi poţi construi cu uşurinţă im adăpost mai bun, pentru a te proteja de tot acest haos. De asemenea, DC parcurs, te vei asigura că nu este totul chiar atât de extraordinar, deşi internetul este astfel. În final, vei trage câteva învăţăminte

fără să fi avut de suferit pagube.

James F. Dunnigan 2 decembrie 2002

James F. Dunnigan 328Westl9 thăt. NY, NY 10011.212.929 – 5288 jfdunnigan@aol.com

Lui Emily Mulcahy, care a fost mult prea raţională pentru a se implica în toate acestea

PREFAŢĂ

Această carte este scrisă pentru publicul larg, cu toate că ea cuprinde multe informaţii istorice şi câteva puncte de vedere tehnice, pe care comunitatea tocilarilor le va găsi interesante. Una dintre marile provocări în scrierea acestor lucruri a fost să folosesc un limbaj pe înţelesul tuturor. Este imposibil să eviţi folosirea multor termeni tehnici atunci când vorbeşti despre PC-uri şi internet. Din acest motiv, la începutul fiecărui capitol se află un mic glosar, şi toţi termenii de aici sunt reluaţi la sfârşitul cărţii. Deşi am depus un mare efort pentru a folosi limba engleză, şi nu pe cea a tocilarilor, acest lucru a fost îngreunat de faptul ca tehnologia internetului este mult mai uşor de explicat în limba tocilarilor. Dar o asemenea concizie ar fi pe înţelesul a numai zece la sută din populaţie. Aşa că dacă nu înţelegi în totalitate o descriere tehnică prezentată aici, nu îţi face griji.

Eşti pe aproape.

Limbajul tehnic imposibil de evitat ne aminteşte că internetul şi P.C.-urile (aşa cum sunt ele proiectate în prezent) nu vor deveni niciodată „aparatură electronică”. În cele din urmă, toată această tehnologie operaţională şi comunicaţională va deveni la fel de simplă şi de puţin controversată ca aparatele electronice, dar atunci când se va întâmpla li est lucru, ele nu vor mai fi „computere personale”. Şi apoi, multe dintre aşa-zisele aparate electronice nu sunt atât de simplu de utilizat pe cât ar vrea

producătorii lor să credem. În mare parte, acest lucru” legătură cu revoluţia în plină desfăşurare a microprocesorului (computerele minuscule de pe un cip, care fac PC-urile să funcţioneze). În prezent, computerele mici sunt integrate în majoritatea aparatelor electronice, ca să nu mai spunem că sunt o componentă-cheie a consolelor de joc, a telefoanelor mobile şi a automobilelor. Unii producători au reuşit să îşi facă produsele controlate de computer atât de simplu de folosit, încât nici nu ne mai dam seama (sau nu ne pasa) că funcţionează cu ajutorul unui microprocesor. Dar tehnologia care avansează cu repeziciune are întotdeauna ceea ce noi, cei care lucram în domeniu, numim „bleeding edge”[1]. Cererea pentru tot ce este mai nou şi mai eficient aduce întotdeauna pe piaţa produse care au o mulţime de detalii neverificate. PC-urile şi mai ales internetul fac parte din aceasta categoric Şi acest lucru nu se va schimba prea curând. Tehnologia ce sta la baza internetului nu numai că este foarte complexa, dar e şi obscură. Nimeni nu ştie cu adevărat ce se petrece cu miile de programe care fac internetul să funcţioneze. Este ca un joc ale cărui reguli sunt în mare parte necunoscute. Oricine descoperă o nouă chichiţă o va putea folosi mereu sau poate ajunge pe prima pagină a ziarelor folosind-o în scopuri rele.

Am trecut de punctul în care principalele victime ale înşelăciunilor pe internet sunt jucătorii important! Băncile, marile companii şi site-urile cu trafic mare au banii şi specialist pentru a se proteja. Acum, cele mai probabile victime suntem noi, ceilalţi, iar această carte încearcă să ne dea şi noua, oameni buni, o şansă în aceasta lupta.

Jim Dunnigan jfdunnigan@aol.com

(şi încă o duzină de alte adrese de e-mail, unele vechi de 20 de ani, o parte dintre ele mai funcţionând şi astăzi…)

---

1 Tehnologii bleeding edge – tehnologii foarte noi, ce prezintă un grad de stabilitate şi de siguranţa incert *(n.red.)*

Mulţumiri

Walter Zacharius este cel care a venit cu ideea, iar Bob Shuman s-a asigurat ca voi face treaba conform programului. De asemenea, aş vrea să mulţumesc câtorva oameni pentru ajutorul oferit la adunarea sau revenirea informaţiilor pentru această carte. Din păcate, niciunul dintre ei nu a dorit ca numele lui să fie tipărit sau asociat cu subiectul cyber-războiului. Cu toate că le-a plăcut cartea, nu au dorit să aibă de-a face cu răzbunarea hackerilor amatori.

CAPITOLUL 1
TU ŞI CYBER-RĂZBOIUL

TERMENI TEHNICI

Glosarul complet, ce include şi termenii definiţi mai jos, poate fi găsit la sfârşitul cărţii.

Bulletin Board System (BBS) este un program pentru computer care permite utilizatorilor să se conecteze la BBS prin modem (în prezent, acest lucru se face prin internet), precum şi să citească şi să scrie mesaje către toate persoanele care utilizează BBS. Versiunea de internet a BBS este Usenet, care are mii de forumuri distincte (pentru subiecte diferite).

Cyber-războinicul este orice specialist militar sau din guvern în domeniul internetului, care ştie cum să atace utilizând reţelele de comunicaţii (cum ar fi internetul) şi să apere reţelele de astfel de atacuri. Începând cu al Doilea Război Mondial, acest tip de activitate a fost numit război electronic. Când este implicat internetul, de multe ori Uni cooptaţi şi voluntari civili pentru a duce acest război. **Atacul DDOS** (Distributed Denial of Service Attack) foloseşte mai multe calculatoare pentru a trimite cantităţi mari de date către un Site-urile pot face faţă doar unui număr limitat de utilizatori conectaţi simultan. În mod normal, aceasta nu este o problemă, dar dacă acaparezi în mod intenţionat toată capacitatea unui site, ca într-un atac DDOS, nimeni altcineva nu mai poate folosi acel site.

Server – un computer pe care sunt stocate site-urile web. Un server este adesea doar un PC ca acela pe care îl folosim acasă, cu un soft special şi o conexiune foarte rapidă la internet. Practic, orice PC poate fi transformat într-un server cu software-ul potrivit şi o conexiune directă la internet (care este destul de scumpă).

Sysadmin este prescurtarea de la System Administrator – administrator de reţea. Acesta este persoana responsabilă de funcţionarea unui site, a unei reţele locale (Local Area Network – LAN) sau a serverului. Nu este o muncă uşoară, întrucât există o mulţime de lucruri care pot merge prost, iar software-ul cu ajutorul căruia funcţionează serverul, site-ul sau reţeaua locală trebuie să fie mereu actualizat pentru a funcţiona în continuare şi a-l proteja de intruşi. Nu sunt niciodată suficient de mulţi administratori de reţea bine pregătiţi şi acest lucru face ca o mulţime de site-uri să fie foarte vulnerabile la atacurile hackerilor.

Zombie este un program cu ajutorul căruia hackerii infectează computerele slab protejate (server ce administrează un site sau un PC cu conexiune la un modem de cablu sau DSL). Există zeci de programe zombie diferite, dar ceea ce au în comun este abilitatea de a comunica cu hackerii pentru a prelua, într-o anumită măsură, controlul asupra computerului pe care l-au infectat. Programele antivirus pot detecta şi elimina programele zombie.

Suntem în război. Şi nu este vorba despre Afganistan, nici despre războiul împotriva terorii. Este un război purtat pe internet. Şi mulţi dintre voi au fost deja, probabil, victime ale hărţuielilor care au loc în fiecare zi. Se numeşte cyber-război şi a reuşit să îi îngrijoreze chiar şi pe generali şi pe politicieni. Pentru că este genul de război care poate pătrunde în orice casă conectată la internet, sute de milioane de utilizatori ai acestuia au, de asemenea, motive de îngrijorare.

Cyber-războiul utilizează reţelele electronice, precum şi informaţiile drept arme. Sau, mai bine zis, ca parte a unei maşini de război. Această formă de cyber-război are loc de mult timp, întrucât avioanele de război foloseau războiul electronic pentru a scăpa de avioanele de interceptare şi de rachetele inamice. De cele mai multe

ori, ne gândim la cyber-război ca la ceva care are loc doar pe internet. Dar nu întotdeauna se întâmplă aşa, mai ales atunci când este implicată şi armata. Un exemplu destul de recent poate fi găsit în Războiul din Afganistan, la sfârşitul anului 2001. Cyber-războiul (spargerea serverelor bancari şi a celor pro-talibane) a fost, de asemenea, combinat cu războiul informaţional (folosind ştirile şi informaţiile ca armă). Tipic secolului XXI. Dar, după cum va fi descris în continuare, războiul informaţional există de mii de ani, iar cyber-războiul, de mai bine de un secol. Ce diferă cu adevărat este probabilitatea ca viitorul cyber-război să-ţi viziteze şi propriul PC.

VEŞTI BUNE, VEŞTI RELE

Cyber-războiul nu este o situaţie chiar atât de sumbră. Există şi veşti bune. Dar, mai întâi, veştile proaste. Da, au loc o mulţime de spargeri ale reţelelor. Mulţi dintre voi s-au ales cu viermi şi viruşi periculoşi de pe e-mail, care în unele cazuri v-au afectat PC-ul. Chiar şi site-urile m. în sunt lovite, la fel ca şi părţi ale infrastructurii internetului. Rezultatul este că, uneori, nu puteţi ajunge pe web acolo unde vreţi. Mai rău decât atât este că analişti ca mine apar în faţa unei camere de filmat şi vorbesc despre evenimente chiar mai cumplite. Într-adevăr, teoretic posibil să produci pagube masive internetului, calculatoarelor, firmelor, agenţiilor guvernamentale şi unităţilor militare conectate la internet. Dar, în acelaşi timp, este foarte, foarte uşor să eviţi să ajungi victimă. La sfârşitul ultimului capitol al acestei cărţi, este descrisă calea spre siguranţă (relativă).

Persoanele cele mai vulnerabile de pe internet sunt cele cu conexiuni rapide şi mereu activate (modem de cablu sau DSL). PC-urile sunt ca nişte magneţi pentru hackeri. Asta deoarece aceste PC-uri sunt în general neprotejate, exact tipul de computere asupra cărora cyber-războinicii şi hackerii preferă să preia controlul. Marile

site-uri, precum şi reţelele corporatiste şi-au luat măsuri de protecţie pentru că au banii şi interesul necesare pentru a face acest lucru. De exemplu, din 11 septembrie 2001, a fost semnalat faptul că mulţi hackeri din Orientul mijlociu au încercat să pătrundă pe site-urile centralelor energetice americane însă fără prea mare succes. Centralele energetice au operaţiuni pe internet bine protejate şi au echipamentul necesar pentru a detecta atacatorii şi locul de unde aceştia operează. Dar milioanele de utilizatori casnici care au conexiuni rapide nu au nicio modalitate de a se proteja în aceeaşi măsură. PC-urile sunt locurile ideale de pe cyber-războinicii îşi pot lansa atacurile. Dacă hackerii din Orientul Mijlociu nu pot pătrunde în centralele de energie nucleară, ei pot, în schimb, să implanteze programe zombie în mii de PC-uri ale utilizatorilor casnici şi pot lansa atacuri DDOS asupra site-urilor militare, comerciale sau guvernamentale, pe care le pot bloca zile la rând. De fapt, un atac într-adevăr masiv ar putea să blocheze părţi importante ale internetului pentru perioade chiar mai lungi decât atât, întrucât remediile pentru atacurile la scară largă nu au fost încă testate în „condiţii de luptă”. PC-urile zombie care se află în case şi nu în instituţii sunt o slăbiciune majoră a internetului şi cel mai probabil câmp de luptă în viitorul apropiat. Cyber-războinicii răuvoitori pot folosi PC-urile expuse pentru tot felul de înşelăciuni. Există o mulţime de alte puncte slabe, dar niciunul la fel de grav ca acesta.

Totuşi, înainte să scoţi din priză propriul PC, trebuie să ştii că există şi câteva veşti bune.

Internetul este o fiară uriaşă în continuă schimbare şi, din fericire, nu se poate iniţia un atac major asupra ei fără o hartă. Astăzi, nimeni nu recunoaşte că ar avea o astfel de hartă. Acest lucru nu înseamnă însă că ea nu ar exista. Probabil că există, dar este considerat secret militar. Spre deosebire de hărţile militare, versiunile

internetului sunt mai mult ca şi cum ai scrie pe cer, fiind în mod constant distorsionate de vântul schimbării care propulsează internetul. Date fiind milioanele de site-uri importante, cele peste două miliarde de pagini web şi milioanele de programatori, administratori de reţea şi colaboratori care modifică în mod constant conţinutul internetului, harta oricui nu ar fi decât un document strict temporar. Mai multe naţiuni recunosc faptul că au mii de militari şi civili care lucrează la astfel de proiecte ale cyber-războiului, dar este un efort continuu, pentru că este nevoie de toţi aceşti oameni doar pentru a păstra harta oarecum la zi. Fără o cunoaştere exactă a ceea ce este acolo, armele cyber-războiului sunt mult mai puţin eficiente.

Din cauza misterului ce înconjoară cartografierea militară a internetului, nimeni nu ştie cât de departe s-a ajuns în crearea şi ţinerea la zi a unei astfel de hărţi. Este cunoscut faptul că, dacă conectezi un nou server la internet, în numai câteva ore îl vor testa diferite organizaţii necunoscute. Şi dacă faci să pară că acel server are o funcţie militară sau guvernamentală, aşteaptă-te să ai parte de alte câteva vizite mai serioase în următoarele zile.

Nimeni nu ştie sigur dacă această atenţie imediată acordată serverelor noi este rezultatul unor operaţiuni militare, dar se ştie că ţinerea în evidenţă a obiectivelor militare valoroase este o procedură standard de operare. Cine face toată această examinare? Există mai mulţi suspecţi probabili. SUA, China, Taiwan şi Japonia, pentru a numi câţiva, au anunţat formarea de unităţi cyber-războinice. Cu toate acestea, există, de asemenea, milioane de oameni care îşi pierd timpul explorând internetul şi spărgând site-uri care li se par interesante şi vulnerabile. Acest lucru este acum considerat un hobby, în ciuda legalităţii îndoielnice a unora dintre aceste activităţi. Dacă echipezi noul server cu instrumente eficiente pentru

detectarea intruziunilor şi pentru monitorizare, poţi afla cine îţi adulmecă site-ul. Urmele unora dintre aceste iscoade vor duce până la baze cunoscute de cyber-războinici din alte ţări, dar majoritatea vor veni din toate colţurile lumii. Aceştia ar putea fi script kiddies1, companii de marketing sau pasionaţi de domeniu. Există foarte mulţi oameni curioşi pe net, pentru o mulţime de motive diferite.

Script kiddies vor doar să îţi folosească serverul sau PC-ul pentru propria distracţie. Comercianţii vor să te cunoască şi să te exploateze, şi, de asemenea, pasionaţi de domeniu destul de inofensivi care pur şi simplu sunt curioşi să afle mai multe despre internet şi care de obicei sunt doar curioşi. Dar în cazul unui conflict, cyber-războinicii vor să îţi folosească PC-ul drept câmp de luptă. Monitorizarea permanentă a internetului în căutare de noi descoperiri face parte din vechea tradiţie militară a spionajului şi este foarte utilă. În acest caz, cyber-războinicii iese mai multe servere slab protejate şi PC-uri „întotdeauna pornite". pentru stocarea cyber-armelor şi a altor instrumente. Dacă PC-ul sau serverul tău îndeplineşte criteriile lor, eşti trecut pe o listă (după care eşti monitorizat periodic) sau eşti dat imediat în folosinţă.

Cyberi-războinicii trebuie să îşi testeze în permanenţă instrumentele şi armele şi, totodată, să îşi antreneze trupele. PC-ul tău poate face parte dintr-o tabără militară de pregătire cibernetică sau dintr-un exerciţiu de instrucţie. Probabil nu vei afla niciodată dacă e aşa. Una dintre cele mai importante abilităţi pe care trebuie să şi le însuşească un cyber-războnic este să fie invizibil.

Să reuşeşti să ataci prin surprindere şi să scapi neobservat este o armă valoroasă.

ADUCEREA RĂZBOIULUI ÎN PROPRIA CASĂ

Da, următorul război va avea loc pe un nou câmp de luptă: propria ta casă. Cyber-războiul este lupta pentru

supremaţia asupra internetului şi a marelui segment din economie care acum depinde de această reţea de computere. Sunt incluse aici şi computerele pe care le folosim acasă. Au avut loc deja încăierări. Viruşii şi viermii informatici despre care ai auzit sunt numai câteva dintre armele folosite pentru blocarea computerelor, distrugerea datelor şi provocarea de stricăciuni centralelor energetice, fabricilor unei naţiuni, aprovizionării cu combustibili, sistemului de comunicaţii şi chiar unor părţi ale forţelor armate. Cea mai mare parte a armelor utilizate până acum au fost folosite de către amatori. Unităţile guvernamentale de cyber-război dezvoltă în permanenţă instrumente şi mai puternice pe care plănuiesc să le folosească la scară largă. Nu poţi observa aceşti superviruşi şi viermi foarte periculoşi până când nu izbucneşte un cyber-război, pentru că, odată ce aceştia sunt descătuşaţi, victimele pot crea un antidot. Dar atunci când vor fi eliberate pentru prima dată, armele internetului vor provoca pagube imense. Taiwan s-a lăudat că deţine un arsenal de o mie de viruşi informatici cu scop de atac. În 2001, doar trei viruşi au cauzat peste 60% din atacurile cyber-războinice de pe internet raportate în acel an. Se cunoaşte faptul că organizaţiile teroriste investighează acest aspect în vederea atacurilor proprii. De menţionat este faptul că prima armă cyber-războinică pentru infestarea unui număr mare de computere (virusul Brain) a fost creată în Pakistan, în anii ’80. Această ţară are încă mulţi programatori talentaţi şi experţi în internet. Cei mai mulţi dintre ei nu caută decât să obţină o viaţă mai bună. Dar sunt şi unii care susţin radicalismul islamic şi organizaţii precum talibanii sau al-Qaeda. Acum poţi înţelege de ce guvernul SUA deţine mai multe variante de internet separate, complet independente de cea pe care o folosim cu toţii. Această operaţiune costisitoare este justificată, pentru că acordă o mai mare protecţie utilizatorilor militari ai internetului.

De ce ar putea deveni computerul pe care îl ai acasă

parte a câmpii lui de luptă cibernetic? Pentru că una dintre cele mai obişnuite tactici este plasarea programelor zombie în cât mai multe calculatoare cu putinţă. Odată ce semnalul este trimis, aceşti zombie îţi folosesc computerul pentru a expedia armele ce vor copleşi guvernul, afaceri sau chiar şi unele calculatoare militare conectate la internet. Este mai puţin probabil ca aceste programe să fie detectate atunci când se află pe calculatoare personale.

În fiecare clipă, mii de PC-uri vor adăposti zombie. Programele zombie cu scop militar nu sunt inofensive pentru gazdele lor; ele vor distruge, probabil, datele personale de pe PC-ul gazdă după ce îşi vor fi terminat treaba murdară pe care o au de făcut pe internet.

Hackerii civili fac acest lucru pentru a da lovitura, cyber-războinicii militari o fac pentru a ajuta la câştigarea războiului, pentru a produce pagube maxime economiei şi forţelor armate ale celeilalte ţări.

Există atât de multe programe zombie pe timp de pace pentru că hackerii civili încearcă mereu să se întreacă unii pe alţii în ingeniozitate. (Unii hackeri se laudă cu peste o mie de zombie instalaţi în calculatoarele în care s-au infiltrat.) Unul dintre aceste calculatoare ar putea fi al tău. Cu toate că este mai uşor să stochezi aceste programe în calculatoarele de acasă, dacă reuşeşti să le implantezi pe site-urile militare sau comerciale bine protejate, vei avea parte de mai mult prestigiu. În ciuda faptului că sunt mai multe şanse ca programele zombie să fie descoperite şi îndepărtate nunei când sunt instalate pe site-uri profesioniste, există şi persoane rău-voitoare care nu vor decât să aibă cu ce se lăuda.

La fel stau lucrurile şi cu crearea viruşilor informatici. Dar hackerii sunt cu adevărat atraşi de lucrurile pe care le pot face cu instrumente simple precum motoare de căutare sau programe de e-mail.

De exemplu, un hacker a creat un software micuţ, simplu, dar periculos, pentru a demonstra că securitatea

furnizorului de e-mail, hotmail.com poate fi străpunsă cu doar două linii de cod. Pentru a răspunde la provocare, un alt hacker a venit cu un program care a reuşit acest lucru cu o singură linie de cod. Aceasta spargere permitea autorului să preia contul de e-mail al oricărei persoane. De reţinut că hotmail.com este o operaţiune Microsoft.

Despre acest aspect voi vorbi mai târziu.

Dar nu este tot. În ciuda pericolului evident, tot mai multe activi guvernamentale şi comerciale sunt controlate prin internet. Este mai ieftin şi mai eficient decât să plăteşti tichete pentru trafic şi să verifici evidentele publice, cu toate că acest lucru face ca America să fie cea mai vulnerabilă naţiune atunci când este vorba despre războiul pe internet. Şi, aşa cum adesea s-a arătat, ar fi nevoie de un Pearl Harbor cibernetic pentru a-i trezi pe cei mai mulţi dintre oameni. Totuşi, dintre toate ţările, SUA beneficiază cel mai mult de pe urma folosirii internetului şi, din fericire, au cel mai mare număr de operatori bine pregătiţi. Dar acest lucru nu va fi suficient, în primul cyber-război, pentru a opri un atac asupra Americii şi nimeni nu ştie cât de mari vor fi pagubele suferite.

SĂ TRECEM LA FAPTE

Atitudinea de genul „să trecem la fapte”, din perioada de început a internetului, a dat naştere multora dintre problemele de securitate pe care le avem astăzi. În anii ’70 – 80, când a fost creată o mare parte din bazele software-ului pentru internet, securitatea nu reprezenta un motiv de îngrijorare. Comunitatea de pe internet era una mică, în care toţi se cunoşteau între ei. Mai mult decât atât, nimeni nu se aştepta ca acest „software experimental” să ajungă să administreze o reţea la nivel global folosită de câteva sute de milioane de utilizatori. De fapt, toate acestea i-au luat pe toţi prin surprindere. Cine ar fi ştiut?

Această atitudine de ignorare a securităţii şi a

calităţii controlului a fost agravată de două alte descoperiri neaşteptate: calculatoarele personale şi Bulletin Board Systems (BBS-urile). Aceste două fenomene au fost responsabile pentru crearea audienţei enorme pentru internet, odată ce acesta a fost creat de către guvern, care ulterior l-a numit ARPANET şi l-a pus la dispoziţia publicului la sfârşitul anilor ’80. Software-ul pentru PC-uri a fost întotdeauna văzut ca fiind de amatori, ca să spun aşa. Şi la început, o mare parte din el chiar aşa era. Dar utilizatorii de PC nu erau prea interesaţi de acest aspect. Tolerau defectele şi încercau să rezolve problemele. BBS-ul a adunat milioane de contacte în reţea şi în căsuţa de e-mail înainte ca internetul să apară. Aşa că, atunci când a fost lansat software-ul World Wide Web, la începutul anilor ’90, care era mult mai uşor de utilizat, internetul a fost propulsat precum o rachetă. Era prea târziu pentru întări securitatea sau pentru a reduce numărul de deficienţe. Întrucât audienţa internetului a atins jumătate de miliard de utilizatori în anul 2002, putem spune că trecutul s-a întors să ne bântuie.

Internetul a fost construit pentru a supravieţui dezastrelor naturale, catastrofelor şi chiar războaielor. Dar nu a fost creat pentru a supravieţui atacurilor venite din partea a milioane de utilizatori răuvoitori. De unde provin toţi aceşti oameni de rea-credinţă? Crackerii şi hackeri black hat (tipii răi) vin din acelaşi loc ca şi tipii buni. De peste tot.

Internetul a facilitat relaţionarea oamenilor cu idei şi intenţii comuni în trecut ar fi fost comunităţi mici de programatori peste tot în ţara (sau în lume), care ar fi discutat despre produse noi şi ar fi lucrat izolaţi de ceilalţi. Acest lucru s-a schimbat pe măsură ce tot mai mulţi dezvoltatori de software au început să folosească ARPANET. Această capacitate de a intra în contact cu oameni cu aceleaşi preocupări, aflaţi în locuri îndepărtate, a fost ameţitoare. Dintr-odată, nu mai erai un simplu

tocilar printre ceilalţi din cartier, ci parte a unei hoarde virtuale de tocilari la nivel mondial. Era o chestie copleşitoare, dar nimeni nu a anticipat că, în cele din urmă, băieţii răi îşi vor forma şi ei propria organizaţie la nivel global.

CINE SUNT TIPII RĂI ŞI CU CE SE OCUPĂ EI

Odată ce numărul utilizatorilor de internet a ajuns la câteva milioane (în anii ’80), cei care voiau să-i pricinuiască pagube au început să se descopere unii pe alţii pe net. Şi apoi au pus în practică ceea ce fac, de obicei indivizii răuvoitori şi cu comportament asocial: vandalizare în masă şi distrugere lipsită de raţiune. În vreme ce efectele comunităţii virtuale au accelerat crearea multor lucruri bune pe internet, le-au permis în acelaşi timp şi celor cu gânduri de distrugere să se reunească şi să îşi construiască armele într-un mod mai eficient. Ani la rând s-a crezut că primii cai troieni şi viruşi răspândiţi pe net pentru a distruge informaţiile oamenilor era rezultatul muncii unor singuratici demenţi. În cele din din urmă, s-a constatat că până şi singuraticilor le place să se întâlnească, iar posibilitatea de a face acest lucru în mod anonim, prin intermediul e-mailului şi al chatului, a avut priză la cei mai mulţi dintre cei interesaţi de vandalismul pe internet. Crearea de software periculos a devenit un efort de grup ce a avut drept rezultat un război şi mai distructiv.

Pentru a înţelege mai bine ce distrugeri pot face tipii răi pe internet, trebuie să înţelegi vocabularul acestui gen de război:

Caii troieni sunt programe deghizate în programe legale. Cineva poate modifica un program care, de exemplu, îţi spune în ce zi a săptămânii a căzut o dată oarecare în ultimele două sute de ani.

Modificarea adaugă o funcţie care poate face ceva interesant sau ceva periculos. Înainte de apariţia

internetului, caii troieni erau o formă enervanta de vandalism de care trebuia să te fereşti.

Existau mai multe variaţii, dar ideea de bază din spatele lor era să capeţi pe PC un program de care nu ştiai sau pe care nu îl doreai. La început, caii troieni au fost folosiţi în scop de farse şi realizau doar nişte glume inofensive (de exemplu, nişte gândaci ce mişunau pe ecran). Dar pe parcursul anilor ’80, aceştia au devenit periculoşi; unii dintre ei distrugeau date sau programe. Alţii, odată rulaţi, se răspândeau prin modificarea altui software cu ajutorul propriilor rutine. Cam în aceeaşi perioadă, creatorii de cai troieni au început să transmită rapid software-urile lor infestate prin sistemele BBS. înainte de asta, cei mai mulţi oameni nu erau online; astfel, cea mai mare parte a software-urilor era transmisă prin dischete. Odată ce BBS-ul a devenit popular, distribuţia a fost mai rapidă, iar caii troieni au ajuns pe (noile) unităţi de hard disk. Din toate acestea s-a născut industria de software antivirus. Şi totuşi, cei mai mulţi utilizatori de PC nu se complică folosind programe antivirus.

Viruşii sunt ceea ce au devenit caii troieni. Virusul se ataşează de un program sau document autentic în anii ’90, când caii troieni au început să se răspândească rapid pe internet, au fost numiţi viruşi informatici. Acest termen era unul corect, în concordanţă cu definiţia medicală a organismului (precum gripa), care se alipeşte de un alt organism mai mare şi mai complex (ca tine) şi foloseşte noua gazdă pentru a produce pagube şi pentru a se înmulţi. Nu toate virusurile care atacă omul sunt dăunătoare, unele fiind chiar folositoare. Dar de acestea auzim foarte rar. Cam din aceleaşi motive, auzim numai despre viruşi informatici periculoşi.

Viermii sunt viruşi care se ataşează de alte programe. De exemplu, Logic Bomb. Acesta este un program ascuns din sistemul computerului care devine activ numai când sunt îndeplinite anumite condiţii. În acel

moment, Logic Bomb se declanşează şi face ceva. De obicei, ceva foarte rău. Acest tip de program este inserat, de obicei, de un programator care are acces legal la calculatorul în cauză. Managerii se tem întotdeauna ca nu cumva un programator nefericit (şi concediat de curând) să lase un Logic Bomb care să se declanşeze atunci când el nu mai este prin preajmă pentru a ţine virusul în aşteptare. Atunci când totuşi se declanşează, cauzează lucruri neplăcute, precum ştergerea evidenţei statelor de plată, sau produce daune mai subtile în evidenţa afacerilor.

Zombie (uneori numiţi şi *boţi,* de la *roboţi)* sunt o variantă a calului troian. Spre deosebire de adevăratele programe cal troian, zombie sunt mai degrabă controlaţi (pe internet) de către persoana care i-a inserat, decât să fie lăsaţi să funcţioneze automat. Sunt programe puternice, care îi furnizează intrusului o serie de facilităţi. Cele mai obişnuite însuşiri ale acestuia sunt înlesnirea accesului la calculatorul invadat, capacitatea de a lansa atacuri de pe acesta, accesul la un chat room protejat de parolă şi stocarea documentelor intruse (software furat, pornografie, instrumente de hacking). Multe alte particularităţi sunt permanent inventate în zecile de programe zombie disponibile pe internet.

Vampirii sunt viermi sau viruşi al căror unic scop este să pătrundă atât de adânc în sistem, încât calculatorul infestat să nu mai poată face nimic altceva. Rezultatul este similar cu ceea ce se întâmplă atunci când ai deschis prea multe programe în acelaşi timp pe PC; lucrează foarte anevoios. Un vampir care rulează pe un server web garantează că cei mai mulţi dintre cei care încearcă să intre pe diverse site-uri de pe acel server vor renunţa, pentru că acesta a încetinit serverul prea mult.

Adulmecătorii sunt instrumente de hacking care colectează informaţiile ce intră sau ies dintr-un computer (de obicei un server). Informaţia este trimisă către cel care a implantat adulmecătorul. Adulmecătorii sunt utili pentru

colectarea parolelor sau a ID-urilor utilizatorilor.

Buffer Overflow Exploitation este o tehnică prin care trimiţi un anumit tip de date către un server web şi declanşezi manifestarea unei deficienţe a software-ului (comună multor produse Microsoft), lucru care îţi permite să strecori un virus sau un program zombie şi astfel să pătrunzi în server, în ciuda apărării. Există o mulţime de alte tipuri de care pot fi exploatate în acest fel. Atunci când ele sunt descoperite, producătorul software-ului tinde să furnizeze rapid o rezolvare. Dar uneori durează mai mult şi, între timp, se produc pagube.

O temere majoră în rândul cyber-războinicilor este că inamicul va fi primul care va găsi o astfel de deficienţă şi va ţine acest lucru secret. Dacă nu se mai împiedică nimeni altcineva de acesta, cei care ştiu de existenţa sa deţin materialul pentru o cyber-armă puternică.

Exista şi alte instrumente de hacking şi arme, dar deja ai înţeles care este ideea.

CYBER-RĂZBOIUL

Încă nu a avut loc un cyber-război. Au existat multe ambuscade, dar niciuna nu s-a apropiat de ceea ce ar însemna o bătălie în câmp deschis pe internet. Cum ar arăta primul cyber-război? Să fim cinstiţi, nimeni nu ştie cu adevărat. Dar pornind de la cyber-armele despre care ştim că există şi de la cele care teoretic ar putea exista, ne putem forma o imagine de ansamblu.

Un cyber-război reuşit depinde de două lucruri: mijloace şi vulnerabilitate. Mijloacele sunt oamenii, instrumentele şi cyber-armele de care dispune atacatorul. Vulnerabilitatea reprezintă măsura în care economia şi armata inamice folosesc internetul şi reţelele în general. Nu ştim cu exactitate cine are capacitatea de a duce un cyber-război, deşi China şi SUA au instituit în mod public unităţi cyber-războinice şi ambele naţiuni beneficiază de o mulţime de experţi în internet talentaţi.

Vulnerabilitatea este o altă problemă. SUA sunt cele mai expuse în faţa unui cyber-război, pentru că, la nivel de naţiune, foloseşte internetul mai mult decât oricare altă ţară. Aceasta este vestea proastă. Vestea bună este că, dacă un atacator ar încerca vreodată să declanşeze un cyber-război prin atacarea SUA, ar putea da greş. Este un risc ce trebuie luat în calcul, atunci când te gândeşti la ce ai putea obţine printr-un cyber-război. Adu-ţi aminte de istoria militară. Atacul de la Pearl Harbor din 1941 s-a întors, de fapt, împotriva japonezilor, prin înfurierea americanilor şi stârnirea unei riposte sângeroase care a lăsat Japonia în ruine. Morala înfruntării de la Pearl Harbor este că, dacă tot vom lovi pe cineva în acest fel, am face bine să-l şi doborâm. Dacă adversarul este mai mare decât tine şi face rost de întăriri, ai putea avea probleme serioase.

Există câteva atacuri cyber-războinice demne de luat în seamă. Desfiinţarea internetului este posibilă, deşi puţin probabilă, pentru că atacurile ulterioare pe internet nu ar mai fi posibile. Astfel că orice tip de cyber-război ar putea avea loc, internetul ar fi lăsat în pace sau ar fi ultimul lucru atacat. Un alt scenariu ar fi preluarea accesului la internet dintr-o ţară întreagă, deşi un astfel de atac ar fi o întreprindere formidabilă numai dacă ar fi vorba de SUA. Dar, în acest caz, trebuie spus că Statele Unite se folosesc de mai multe tipuri de internet (internetul obişnuit, patru interneturi guvernamentale izolate şi internet 2, un experiment al următoarei generaţii de internet). Înfrângerea internetului principal nu ar produce pagube prea mari celorlalte reţele, pentru că, în vreme ce economia ar suferi îngrozitor, funcţiile guvernamentale ar fi mai puţin afectate. Asta dacă inamicul nu face un extraordinar efort de penetrare şi atacare a interneturilor guvernamentale.

Deci având internetul încă intact, toate tipurile de mutilare pot fi duse la îndeplinire. Am văzut deja cum

viermii şi viruşii distrug cantităţi imense de date. Acest lucru ar putea fi făcut mai rapid şi la scară mai largă pe timp de război, din cauza numărului mai mare de viruşi distructivi şi a atacurilor lansate în acelaşi timp. Această distrugere ar putea însemna doborârea multor site-uri militare, guvernamentale şi comerciale de maximă importanţă.

Pot fi folosite şi alte cyber-arme, precum atacurile DDOS şi viruşii speciali pentru distrugerea ruterelor sau a altor computere specializate care asigură funcţionarea internetului.

Este important să nu pierdem din vedere faptul că aproape orice server web sau PC conectat la internet poate fi spart. Există multe cazuri de hackeri pe cont propriu sau în grupuri mici care au pătruns în sute de servere într-o perioadă scurtă de timp. Acestea sunt situaţiile în care hackerii sunt prinşi. Ceea ce îi neliniştеşte pe mulţi este faptul că nu putem şti cât de mulţi oameni fac acest lucru fără să fie vreodată descoperiţi. Ştim că există, pentru că unele atacuri sunt constatate la mult timp după ce au avut loc, iar unii dintre hackerii arestaţi oferă detalii despre unele atacuri nedescoperite. Unul dintre motivele pentru un multe atacuri trec neobservate pe timp de pace este că există mai multe şanse ca un site anonim să fi picat din cauza rateurilor obişnuite (defectarea hardware-ului ori a software-ului sau o eroare umană) ce necesită o resetare a serverului, decât din cauza atacului unui hacker.

De asemenea, rămâne valabil faptul că serverele bine protejate sunt sparte foarte rar, în timp ce vandalismul web este mult mai des întâlnit în cazul serverelor slab protejate. Dar pe timp de război, nu ar exista niciun dubiu că majoritatea problemelor computerului ar fi cauzate de atacurile cyber-războiului. Pagubele şi distrugerile ar fi prea larg răspândite şi intense pentru a fi greşit interpretate.

Dincolo de site-urile web, există o mulţime de

facilităţi industrial şi de comunicaţii a căror funcţionare depinde de computere. Site-urile de transport includ o serie de depouri de cale ferată, care susţin cea mai mare parte a traficului feroviar naţional. Traficul camioanelor poate fi paralizat prin atacarea computerelor care controlează aprovizionarea cu combustibili (rafinării, conducte, rezervoare şi sisteme de distribuţie).

Lovirea acestor ţinte răspunzătoare de combustibil va afecta şi transportul aerian. Zborul aeronavelor comerciale poate fi împiedicat prin pătrunderea în calculatoarele care controlează sistemul de trafic aerian. Sistemele de mentenanţă pentru aeronavele comerciale depind, de asemenea, de reţelele conectate la internet.

Cea mai mare parte a PC-urilor din firmele americane este conectată la un anumit tip de reţea, dar are, de obicei, şi o conexiune la internet. Aşadar, numărul de ţinte posibile este foarte mare, la fel ca şi gradul în care viaţa noastră de zi cu zi ar fi afectată. Multe afaceri pot funcţiona fără computere, dar nu foarte bine şi nu pentru mult timp.

Comunicaţiile noninternet sunt şi ele destul de vulnerabile. Poate că nu intenţionezi să dobori internetul, dar închiderea unor sisteme financiare distincte, precum Rezerva Federală, va îngheţa operaţiunile financiare locale şi internaţionale ale multor companii. Rezerva Federală este perfect conştientă de vulnerabilitatea sistemului de transfer monetar. După ani de pregătire şi de planificare pentru actualizarea reţelei, s-a decis, în martie 2002, schimbarea planurilor şi renunţarea la Microsoft. Sistemele de operare Microsoft erau privite ca fiind prea vulnerabile pentru ceva atât de vital pentru economia naţională precum reţeaua Rezervei Federale.

Pentru toate celelalte operaţiuni, care nu depind atât de mult de internet, este posibilă interferenţa cu infrastructura electrică. Înseşi centralele electrice deţin un oarecare control de la distanţă, în mare parte realizat prin

intermediul internetului. Acelaşi lucru se petrece cu sistemul de distribuţie a electricităţii ce are un număr mic de transformatori de mare putere, care, atunci când sunt folosiţi în mod greşit, sunt avariaţi. Durează luni de zile pentru a construi înlocuitori ai acestor transformatori şi nu există decât câţiva disponibili pentru cele aproximativ două duzini de transformatori ce operează în America de Nord. În cele din urmă, există atât de vulnerabilii sateliţi spaţiali şi staţiile terestre controlate prin computer. Încearcă să împiedici comunicarea cu aceste „păsări" şi vei suspenda navigaţia GPS, monitorizarea vremii, sateliţii-spion şi unele reţele de telefonie şi televiziune.

MARELE NECUNOSCUT

Nimeni nu a încercat vreodată un atac cyber-războinic de mari amploare. Nimeni nu ştie exact cât de vulnerabile sunt ţintele-cheie descrise mai sus. Nu uita, inamicul ar trebui să depisteze erori de care oamenii ce administrează aceste ţinte nu sunt conştienţi. Cei care gesnonează un site au avantajul că deţin controlul absolut asupra serverelor proprii. Sistemele de securitate ale acestor servere încep să fie schimbate şi actualizate în mod regulat, îngreunând astfel lucrurile pentru oricine ar plănui un asalt cibernetic. Atacatorul ar avea parte de multe atacuri eşuate, pentru că, în timpul scurs între planificarea atacului (bazat pe informaţiile adunate cu săptămâni sau luni în urmă) şi ducerea lui la bun sfârşit, au avut loc prea multe schimbări la serverele – ţintă.

Adversarul cu cele mai bune informaţii despre starea internetului, mai ales a fiecărui site-cheie inamic, va avea succes. Cyber-războinicii profesionişti plănuiesc să îşi declanşeze armele atunci când este limpede vor avea sorţi de izbândă. Acest lucru înseamnă că mai multe cyber-războaie vor avea loc sub forma unor războaie mai mici, chiar şi atunci când nu este declarat niciun război. Până acum, acest lucru s-a întâmplat în SUA, mai ales prin

exploatarea unor reţele wireless populare în mai multe ţări mai puţin industrializate.

În reţelele wireless se poate mult mai uşor şi se pot face mai multe manevre. Acest lucru a dat roade în Războiul împotriva Irakului în 1991 şi Serbiei în 1999. Războiul împotriva terorismului presupune multă muncă de detectiv pe internet, iar războiul din Afganistan a luat repede sfârşit datorită abilităţii forţelor americane de a crea rapid în această ţară reţele wireless de voce şi de date.

Deşi acest lucru nu a fost menţionat la vremea respectivă, aceste reţele erau pregătite să reziste eventualelor încercări de hacking. Asemenea atacuri nu au avut loc niciodată, dar trupele erau pregătite.

Alte naţiuni consideră că este util să fure date valoroase de pe numeroasele site-uri comerciale, guvernamentale sau militare din America. Aceasta este de fapt, o formă de cyberspionaj şi are loc de mai multe generaţii încoace. Dar cu ajutorul internetului şi al numărului mare de alte reţele folosite astăzi, oportunităţile de spionaj electronic sunt mult mai mari în prezent. De vreme ce spionii nu vor să fie detectaţi (ca să se întoarcă mai târziu pentru mai multe secrete), acest spionaj are şi rolul de a analiza eventualele atacuri cyber-războinice care ar putea produce pagube.

În ceea ce priveşte internetul, numai ţările industrializate depind în mare măsură de el. Din acest motiv, Japonia şi Coreea de Sud sunt mai îngrijorate de un atac cibernetic din partea Coreei de Nord decât viceversa. Acest lucru face ca atacul împotriva unei naţiuni puternic dependente de internet să fie mai costisitor. Iar această dependenţă nu va face decât să crească, întrucât este limpede că utilizarea masivă a internetului duce la dezvoltare economică.

CELE MAI PROBABILE CYBER-RĂZBOAIE

Armele nucleare au împiedicat marile naţiuni să meargă la război una împotriva celeilalte în ultima jumătate de secol. Probabil că acest lucru va continua. Dar cyber-războiul oferă oportunitatea de a duce un război anonim împotriva altei ţări. Acest lucru s-a mai făcut în trecut, în mare parte prin susţinerea tacită a opoziţiei sau a grupurilor teroriste din ţările inamice. Secretul este să îţi ascunzi urmele. Se crede că virusul Code Red, apărut în anul 2001, care încă produce pagube foarte mari, a venit din China, dar China neagă orice amestec în apariţia lui. Code Red a cauzat mult mai puţine daune în China, pentru că acolo sistemul de operare folosit în mod curent este Linux, în vreme ce virusul ataca numai PC-uri care utilizau software Microsoft. Asta face ca unei naţiuni precum China să îi fie mai uşor să lanseze cyber-atacuri împotriva SUA, fără să se teamă de represalii care i-ar putea afecta infrastructura de internet în plină dezvoltare. În China, spre deosebire de alte ţări ostile Americii (Coreea de Nord, Irak, Iran), internetul este în creştere. China are, de asemenea, mii de programatori talentaţi şi a recunoscut că pregăteşte unităţi militare pentru dezvoltarea şi utilizarea cyber-armelor. Aşa că data viitoare când vor exista tensiuni între SUA şi China este posibil ca americanii să se confrunte cu nişte cyber-atacuri periculoase şi greu de depistat. Singura problemă căi eu China trebuie să îi facă faţă în acest caz este că eventualele victime colaterale ale unui potenţial atac pe care l-ar declanşa vor conduce la înrăutăţirea anumitor relaţii diplomatice. Chiar şi în cazul în care atacurile lansate numai asupra Americii nu ar fi asociate Chinei, aceasta din urmă tot ar fi suspectul principal. S-ar crea o situaţie în care Chiina ar fi singura ţară care ar avea şi motivele şi mijloacele necesare. Bine înţeles că ar putea oricând să strecoare Irakului, Iranului sau Coreei de Nord un CD cu diferite arme cibernetice şi să aştepte ca aceste naţiuni să lovească America. La rândul lor, chinezii sunt fără îndoială con. şi ieri că

America şi-ar putea lansa propriul cyber-atac anonim împotriva Chinei. Efectele unui asemenea război sub acoperire nu ar putea fi ascunse, cum nu ar putea fi ascunsă nici disperarea diplomaţilor de a duce acest război nedeclarat la bun sfârşit. Lucrurile se vor petrece chiar aşa.

Există şi teama că teroriştii vor încerca un atac major pe internet. Acest lucru nu s-a petrecut încă. Sunt o mulţime de oameni inteligenţi, experţi în internet, care fac parte sau simpatizează cu organizaţiile teroriste. Se ştie că foarte multe grupări teroriste utilizează în mod frecvent internetul. Osama bin Laden şi al-Qaeda s-au folosit foarte mult de internet (şi au recunoscut acest lucru public înainte de 11 septembrie 2001). Lipsa atacurilor teroriste pe internet este, de fapt un indiciu al gradului de înzestrare umană de care este nevoie pentru a crea şi executa un atac autentic. Nu uita că, odată ce un nou virus este creat şi lansat sau vulnerabilitatea nou descoperită a unui ne este exploatată, site-urile importante (cele care i-ar atrage cel mai mult pe terorişti) sunt de obicei primele care îşi întăresc apărarea. Îndepărtarea unui atac cibernetic ce ar putea produce pagube necesită i tehnologie. Fără îndoială, o organizaţie teroristă ar reuşi, în cele din urmă, să formeze un asemenea grup, lucru ce ar putea avea îngrozitoare. Mai e mult sau nu până se va întâmpla astfel? De reţinut este faptul că, spre sfârşitul anului 2001, exista o creştere sesizabila a monitorizării şi testării centralelor energetice ale SUA şi Europei. Se pare că cineva încerca să pătrundă într-o centrală energetica şi s-o atace cibernetic.

Ameninţarea teroristă actuală vine din ţările islamice şi arabe, care are cele mai puţin dezvoltate resurse (în ceea ce priveşte utilizarea şi experţii în internet). Dar dacă teroriştii dispun de bani, există nenumărate bande criminale care ar înfrunta pe oricine. Există, de asemenea, posibilitatea ca în urma unui efort de spionaj să se obţină o

parte din armele informatice militare (în special viruşi şi alte cyber-arme). La sfârşitul Războiului Rece, atât Rusia, cât şi SUA au fost surprinse de numărul de trădători, de ambele părţi, care au făcut asta pentru bani.

Este puţin probabil ca teroriştilor islamici să le fie furnizate cyber-arme de către China, întrucât aceasta are propria minoritate islamică ce lupta împotriva dominaţiei chineze. Dar din moment ce China deţine cyber-arme care nu pot fi folosite cu adevărat decât împotriva ţintelor americane, cine ştie ce s-ar putea întâmpla?

SUSPECŢII DE SERVICIU

Cei care produc cea mai mare parte a daunelor pe internet sunt fie un număr mic de infractori, fie un număr mare de adolescenţi neastâmpăraţi sau anarhişti bizari care deţin computere. Cyber-infractorii sunt doar o mână de oameni, câteva sute de persoane. Cei mai mulţi dintre ei se specializează în escrocherii ce nu presupun tehnologie avansată, ci doar folosirea unui număr mare de spamuri sau pagini web maliţioase. Câştigurile fabuloase (mai mult de 100.000 $) de pe urma unor astfel de infracţiuni sunt la ordinea zilei. Cele mai multe dintre pierderile provocate de infracţionalitatea cibernetică se traduc prin plata pentru muncă depusă în vederea restabilirii funcţionării normale a site-urilor web afectate şi a afacerilor pierdute cât timp aceste site-uri n-au putut fi accesate. Apropo, companiile sunt mai dispuse să calculeze şi să anunţe aceste pierderi decât să facă publice furturi mari de bani.

Chiar şi înainte de apariţia internetului, marile instituţii financiară obişnuiau să ascundă astfel de furturi (şi să înghită pierderile), nedorind să rişte pierderea încrederii publicului. Această atitudine se dovedeşte a fi problematică pentru poliţie şi FBI. De fapt, FBI face presiuni pentru o lege care să permită companiilor să declare eventualele spargeri, fără teama că informaţia ar

putea ajunge în presă. Din nou vedem cum războiul informaţional este strâns legat de cyber-război.

Cei mai vizibili infractori informatici sunt numeroşii script kiddies şi atacatorii mărunţi care utilizează instrumentele de hacking şi de furt deja existente pe internet. Acest grup produce un puternic zgomot de fond. Dacă monitorizezi un detector de intruziuni de pe un server (sal chiar şi pe PC-ul tău), vei vedea o mulţime de scanări şi de testări.

Cu puţin antrenament, poţi învăţa să deosebeşti activităţile profesioniştilor şi bruiajele haotice generate de amatori. Practic, hackerii profesionişti se vor ascunde în spatele celor neexperimentaţi. Exista o mulţime de amatori de senzaţii tari care sunt relativ inofensivi; îşi petrec majoritatea timpului navigând pe internet fără să ştie prea bine ce fac. Hackerii profesionişti nu vor ţinti calculatorul personal, dar amatorii s-ar putea să o facă. Nu este însă deloc plăcut ca vreunul dinţii aceşti tocilari în devenire să îţi facă praf hard drive-ul sau îţi blochează conexiunea la internet în timp ce încearcă să închidă site-ul liceului lor.

Este nevoie de cel puţin jumătate, dacă nu de întregul efort a peste zece milioane de oameni pentru a menţine funcţionarea internetului. Cei mai mulţi dintre aceştia ştiu destul de bine cum funcţionează şi li se potriveşte ca o mănuşa celor care sunt distructivi.

Există totuşi o excepţie; hackerii black hat şi acei script kiddies aduc cu ei un element-surpriză. În asta constă toată diferenţa. Dacă cyber-războinicii atacă, băieţii buni îşi vor reveni din mers. Internetul şi oamenii care îl fac să funcţioneze s-au dovedit a fi foarte adaptabili atunci când sunt loviţi cu asalturi majore. Dar această abilitate are preţul ei. Facturile pentru orele suplimentare, ca să nu mai spun despre uzura psihică a tuturor acelor insomniaci, se plătesc scump. Este unul dintre motivele pentru care aproape jumătate dintre cei care devin programatori renunţa la acest domeniu în maximum zece ani. Există şi

modalităţi mai puţin solicitante de a-ţi câştiga existenţa.

Oamenii care vor fi loviţi cu adevărat atunci când (nu dacă) se va declanşa un atac cyber-războinic major sunt sutele de milioane de utilizatori ai internetului. Cei mai mulţi dintre ei nu dispun de echipamentul tehnic necesar (aşa cum dispun companiile şi guvernele) pentru repararea daunelor. Aceia care vor citi cu atenţie ultimul capitol al acestei cărţi vor fi mai pregătiţi să facă faţă unui atac, dar cei mai mulţi utilizatori de internet vad în PC-urile lor nişte dispozitive. Vor doar să le folosească şi să nu piardă timpul cu întreţinerea şi înţelegerea lor.

Un efect posibil al eventualităţii unui cyber-război sau al unui atac terorist pe internet este apariţia companiilor de recuperare de date în urma dezastrului. Exista deja o mică industrie care se ocupa cu aşa ceva, care poate ajuta la recuperarea datelor de pe un hard disk defect sau furnizează experţi în stare să rezolve prin telefon daunele produse de un virus sau de o alta catastrofa pe computer. Dar aceste servicii vor fi scumpe (cel puţin câteva sute de dolari, uneori chiar câteva mii pentru asemenea servicii) şi unele date vor fi pierdute pentru totdeauna, lăsând în urmă frustrări şi neplăceri.

CE SE POATE FACE

Dacă utilizatorii private sunt cele mai vulnerabile ţinte într-un viitor cyber-război, ce poţi face pentru a te proteja? Aşa cum se explica în ultimul capitol, exista câteva lucruri care te vor face mai puţin vulnerabil. Pe scurt ar fi cam aşa (toate detaliile necesare se găsesc în ultimul capitol):

1. Opreşte orice script. De acestea se folosesc în prezent cei mai cunoscuţi viruşi pentru a avaria computerele de acasă sau pe cele de la serviciu. Acest lucru se verifica în primul rând în cazul PC-urilor ce folosesc sisteme de operare Microsoft. E căzut pentru aproximativ 90% dintre PC-uri şi de aceea viruşii sunt

create pentru a ataca software-ul Microsoft. Dar viruşii pot ataca şi computerele MacIntosh sau Unix.

2. Foloseşte un program antivirus. Acesta te va protezia dacă PC-ulntau nu răspunde comenzilor şi suspectezi un virus sau o alta intruziune. De cele mai multe ori, este vorba despre erori de system, dar pentru liniştea ta meritä să iei un program antivirus.

3. Actualizează-ţi software-ul (folosind actualizările gratuite). Cei mai mulţi producători de software facilitează obţinerea acestor actualizări de pe internet.

Şi, în cele din urmă, dacă ai o conexiune rapida la internet (de obicei prin cablu sau prin DSL), instalează un sistem firewall. Tu, prietene, eşti ţinta principal a oricărui viitor cyber-război. Da, ştiu că sunt milioane de oameni ca tine, dar din motive pe care le voi explica mai târziu în carte, PC-ul tău reprezintă punctual zero pentru atacurile iniţiale ale unui cyber-război. Fa rost de un firewall şi probabil vei putea să stai departe de război.

Începând cu următorul capitol, vei afla o mulţime de amănunte uimitoare.

CAPITOLUL 2
ORIGINILE CYBER-RĂZBOIULUI

TERMENI TEHNICI

Glosarul complet, ce include şi termenii definiţi mai jos, poate fi găsit la sfârşitul cărţii.

Baudulul este unitatea de date transferate pe secundă printr-o linie telefonică prin intermediul unui modem. Cu aproximaţie, opt bauzi corespund unei litere sau unei cifre. Aşadar, un modem de 300 de bauzi (din anii ’70) poate transfera aproximativ 37 de caractere pe secundă. Cele mai multe modemuri din ziua de azi operează cu 56.000 de bauzi.

Baza de date este un fişier de pe calculator, de multe ori unul foarte mare, care conţine liste de informaţii (nume, adresă şi alte lucruri pentru toţi clienţii, sau angajaţii, sau orice altceva). Utilizatorii de baze de date folosesc un software special pentru a putea să găsească informaţii în baza de date şi pentru a face actualizări.

FTP, prescurtare de la File Transfer Protocol, este un program de computer care permite utilizatorilor de internet să obţină fişiere (date sau programe) de la un alt computer.

Hackingul îţi foloseşte abilităţile tehnice pentru a lucra la un program sau pe internet. De obicei, intenţia este de a îmbunătăţi modul în care funcţionează software-ul, dar hackerii răi nu urmăresc decât să provoace pagube cât mai mari.

LAN, prescurtare de la Local Area Network, este un sistem necostisitor de software şi cabluri care interconectează mai multe PC-uri într-un birou. LAN-ul în sine este de multe ori conectat la internet, astfel încât toţi utilizatorii LAN pot naviga pe net.

Computerele mainframe sunt cele mai mari, mai

scumpe, mai complexe şi mai puternice calculatoare. Acestea, de obicei, acoperă cele mai multe dintre nevoile de calcul pentru o organizaţie mare. Reţine că primele mainframe-uri ale anilor ’60 au mai puţin de unu la sută din viteza şi capacitatea de stocare a celui mai ieftin PC de azi (de 500 $).

Nodurile sunt unul (sau mai multe) servere (a se vedea definiţia de mai sus) care stochează informaţiile necesare pentru un site.

Cyber-războiul în sine este destul de vechi, numai termenul este relativ nou. Termenul este derivat din *cibernetică* şi a început să fie folosit la începutul secolului XX, pentru a descrie relaţia dintre oameni şi maşinării. „Cyber” este termenul grecesc pentru pilot. Atunci când au apărut computerele, la sfârşitul anilor ’40, cibernetica era un cuvânt la modă, iar „cyber” a devenit un prefix pentru orice avea legătură cu computerele. Până la sfârşitul anilor ’90, puteam auzi termeni noi, precum cyber-management, cyber-şcoală şi cyber-război. Dar termenul de cyber-război se află încă la început. Mai simplu spus, cyber-războiul se referă la utilizarea tuturor instrumentelor de calculator sau electrice disponibile pentru a opri aparatura electronică şi comunicaţiile inamicului. Fără menajamente, este permis orice. Cu toate acestea, nouă în acest domeniu al războiului este utilizarea calculatoarelor şi a altor unelte electronice. Obiectivul, aşa cum a fost vreme de mii de ani, este perturbarea comunicaţiilor inamice. În trecut, aceasta însemna urmărirea mesagerilor inamici sau folosirea unor sunete sonore şi a steagurilor false ale inamicilor pentru a trimite semnale înşelătoare în timpul unei lupte. Acesta este un punct important, pentru că metodele cele mai obişnuite de a duce un cyber-război nu implică computere sau dispozitive electronice. Să furi parole trăgând cu urechea la cineva sau cotrobăind prin birou nu este ceva ieşit din comun. O mare parte dintre aceste acţiuni poartă

azi numele de război informaţional, care se duce în timpul campaniilor politice prin amăgiri, înşelătorii sau minciuni directe. De asemenea, războiul informaţional joacă un rol important în orice cyber-război, pentru că mesajele mincinoase sau distorsionate pot opera prin mai multe canale electronice (radio, TV, telefon, internet).

De-a lungul istoriei omenirii, comunicaţiile au reprezentat întotdeauna o armă esenţială. Capacitatea de a transmite cantităţi masive de informaţii verbale, sau mai târziu scrise, le-a permis oamenilor, în timp, să creeze organizaţii mai mari decât cele identificabile în orânduirea socială a animalelor. Tribul era aproximativ echivalentul unei cirezi său. Îi unei haite. Dar regatul era atât de mare, încât nu putea fi condus în văzul tuturor celor care îl alcătuiau. Conducerea unei organizaţii mari a necesitat noi forme de comunicare. Imperiile antice nu aveau telefon, nici internet, dar foloseau mari reţele de comunicaţie. Amerindienii trimiteau semnale cu ajutorul fumului, iar africanii foloseau tobele. Acum 300 de ani, primele imperii au creat reţele de turnuri care foloseau fumul, focul, steagurile sau chiar semnale vocale pentru a transmite mesaje rapid, de la un turn sau vârf de deal la altul. Cu aceste sisteme, regele sau împăratul putea şti, în interval de o zi, tot ce se petrecea pe o distanţă de sute de mile. Metoda era esenţială pentru a putea conduce un teritoriu atât de mare. Dacă năvălitorii ar fi atacat un anumit teritoriu, ar fi avut puţin timp la dispoziţie pentru a jefui, înainte ca trupele împăratului să îi atace. Simplul fapt că ştiau despre sistemele de comunicare i-a făcut pe mulţi atacatori să păstreze distanţa, iar supuşii rămâneau loiali faţă de conducătorul local, fiind bucuroşi pentru protecţia pe care acest sistem o furniza.

Cu toate acestea, reţelele antice de comunicaţie erau vulnerabile. Un invadator inteligent ar fi trimis iscoade pentru a observa turnurile de semnalizare (sau culmile de deal de pe care inamicul trimitea semnale către alte

turnuri de la mare distanţă). Pe internet, echivalentul ar fi un atac de tip DDOS. Dacă sistemele de comunicaţii ar putea fi distruse, armata invadatoare ar putea provoca multe pagube înainte ca forţele imperiale să fie alertate şi mobilizate. Mongolii, care au cucerit cea mai mare parte din Eurasia în secolele al XIII-lea şi al XIV-lea, erau interesaţi în mod special de distrugerea reţelelor de comunicaţie inamice înainte de atac. Ei înşişi foloseau curieri care băteau ţara în lung şi-n lat în vreme ce armatele lor avansau. După ce cucereau o zonă, mongolii foloseau, la rândul lor, turnurile de semnalizare capturate. Îşi apărau cu ardoare propriile metode de comunicaţie. Protejarea propriei capacităţi de comunicaţie este o strategie-cheie pentru orice cyber-război. Capacitatea de a putea vorbi cu propriile trupe în timp ce inamicul nu poate vorbi cu ale lui are şi a fost întotdeauna un avantaj evident.

Cele mai multe istorii nu menţionează sistemele de comunicaţii, dar fără ele, aceste imperii antice nu ar fi putut supravieţui. Evident că reţelele nu dispuneau de tehnică avansată, dar erau costisitoare şi nu erau prea numeroase. Însă funcţionau. O altă problemă era viteza cu care puteau fi transmise informaţiile. Împăraţii antici erau singurii care îşi puteau permite costurile construirii a mii de turnuri de semnalizare pentru a trimite şi primi rapid mesaje de la sute de mile distanţă. Orice rival posibil al imperiului era nevoit să folosească o comunicare mai înceată (de obicei, un tip călare pe un cal rapid). Informaţiile au reprezentat întotdeauna o armă puternică, iar cel care făcea cel mai repede rost de informaţie era mult mai puternic decât cel care nu reuşea acest lucru.

ALEXANDRU CYBER-RĂZBOINICUL

În urmă cu aproximativ 2.500 de ani, cuceritorul macedonean Alexandru cel Mare a înţeles cum trebuie să îşi comunice planurile prin intermediul cuvântului. În

contextul relaţiilor publice antice, Alexandru şi-a scris propriile comunicate de presă în scrisori oficiale către supuşii săi, uneori rebeli, din Grecia. Faptul de a primi astfel de scrisori de la rege era o noutate şi, întrucât se făceau copii care erau apoi postate în pieţele din toată Grecia, regele era privit ca fiind un tip inteligent şi de succes. De asemenea, Alexandru transmitea directive către noii supuşi persani, care aveau acelaşi efect ca şi scrisorile din Grecia. Baronii mass-mediei moderne sunt perfect conştienţi de necesitatea de a „agita spiritele" pentru a întâmpina aşteptările clienţilor, la fel cum oamenii din trecutul îndepărtat, care nu dispuneau de canale mass-media timp de 24 de ore din 24, erau nerăbdători să afle ştiri. Pe atunci, călătorii ştiau că pot primi o masă gratis, dacă aveau informaţii de dat la schimb. Să răspândeşti veştile nu este deloc un produs al erei cyber-războiului; această tehnică este veche de peste trei mii de ani. Faraonii Egiptului antic aveau propria versiune a evenimentelor, care era în permanenţă pictată sau cioplită pe monumente. Alexandru era conştient de această tehnică, ce i-a influenţat, probabil, modul de gândire. Faraonii gândeau pe termen lung, întrucât acele comunicate de presă monumentale erau înălţate la câţiva ani după ce avuseseră loc războaiele sau luptele descrise. Pentru că nu existau reporteri de investigaţii pe vremea aceea, iar faraonul deţinea monopolul asupra acestui tip de mass-media, versiunile lui au rezistat mii de ani. În plus, egiptenii erau condiţionaţi, după secole de astfel de management al ştirilor, să creadă varianta „oficială" a evenimentelor.

De abia în ultimele zeci de ani au descoperit arheologii răstălmăcirile din spusele faraonilor. De exemplu, acum ştim că faraonul prezenta, uneori o versiune a evenimentelor care, pe lângă faptul că era falsă în privinţa evenimentelor, îl făcea şi pe el să apară mai bine decât ar fi meritat. Cel mai bun exemplu în acest sens

a avut loc în anul 1287 î. Hr., când faraonul Ramses a fost atacat de o armată a hitiţilor la Kadesh (în Siria) şi de abia a scăpat cu viaţă. Ramses s-a întors acasă, a declarat că a obţinut o mare victorie şi a pus ca această versiune să fie pictată pe pereţi şi sculptată pe monumente. Această versiune înşelătoare a bătăliei a fost acceptată până în secolul XX, când arheologii au scos la iveală dovezi care susţin contrariul.

O mie de ani mai târziu, Alexandru şi-a început propria campanie prin care să impună o altă versiune a evenimentelor decât cea reală. Oraşele greceşti care populau estul Mediteranei erau locuite de o populaţie mai educată decât cea a Egiptului antic. Rata de alfabetizare, care era încă de doar 15%, a permis comunicatelor scrise să circule mai repede. Conducătorii greci de dinainte de Alexandru au considerat că este util să afişeze scrisori în centrul zonelor urbane, pentru a raporta activitatea de guvernare. Cele mai multe dintre aceste oraşe erau democratic organizate, aşa că trebuia să îi menţii pe alegători (bărbaţi adulţi, care aveau mai multe şanse să fie cunoscători de carte) de partea ta. Scrisorile erau apoi copiate şi duse în cetăţi sau oraşe mai mici, pentru a fi citite sau rostite în faţa celor care nu ştiau să citească. După standardele egiptene, ştirile circulau în oraşele greceşti cu viteză maximă. Totuşi, chiar şi în acest punct de cotitură din istoria comunicaţiilor, mai importante erau tehnica folosită şi modul în care o utilizai. Când tatăl lui Alexandru, Filip Macedoneanul, a reuşit să cucerească oraşele greceşti în anul 338 î. Hr., el s-a aflat la sfârşitul unui război informaţional. Multor greci nu le plăcea de Filip şi nu îndrăgeau nici ideea de a li conduşi de macedonean. Mulţi dintre aceşti critici erau oameni cu ştiinţă de carte. Filip nu a reuşit niciodată să transforme în mod favorabil toate lucrurile jignitoare pe care grecii le spuneau la adresa lui (cel mai adesea, faptul că nu era grec). În cele din urmă, Filip a fost asasinat (în anul 337 î.

Hr.). Fiul său.

Alexandru, intrase într-o conjunctură periculoasă. Dar încă de la început, el le-a dat oamenilor motive să-l numească „cel Mare”. În timp ce Filip a strivit o mulţime de duşmani cât timp a luptat pentru a cuceri Grecia, Alexandru a intrat în scenă ca un tânăr fără prea multe antecedente. Filip a favorizat trădarea şi crima în masă pentru a obţine ce îşi dorea, în vreme ce Alexandru era mai puţin însetat de sânge şi mai preocupat de imaginea sa publică. De asemenea, era considerat mai degrabă grec decât macedonean. El fusese educat de eminenţi profesori greci şi acest lucru se vedea. Mai mult, Alexandru era, ca şi tatăl lui, o fire foarte activă. Un impostor cu tot felul de propuneri interesante într-o mână şi cu o sabie ascuţită în cealaltă.

Înainte de a ajunge să fie prins cu mâţa-n sac, Alexandru a adunat armata pe care o moştenise (şi pe care nu îşi mai permitea să o susţină) şi a invadat Imperiul Persan. Invadarea unui vecin bogat într-o încercare disperată de a ieşi din problemele politice de acasă este o iniţiativă antică. Dar este şi una modernă. Cu toate că nu a funcţionat pentru Saddam Hussein, în 1991 (datora Kuweitului miliarde de dolari, pe care nu îi putea restitui), a funcţionat pentru Alexandru cel Mare. El şi-a păstrat poziţia de rege în mare parte datorită armatei sale de soldaţi profesionişti. Dar nu avea banii necesari pentru a o plăti. Decât să renunţe la o mare parte a armatei, el a preferat să atace Persia.

Războiul persan s-a terminat mai bine decât Războiul din Golf, pentru că Alexandru era un mult mai bun comandant de armată decât Saddam. Alexandru a câştigat aproape toate bătăliile, spre deosebire de Saddam Hussein, care le-a pierdut pe cele mai multe. Un element ajutător a fost şi faptul că Alexandru a întreprins nişte acţiuni primitive, dar eficiente, de relaţii publice.

Iată cum a procedat: Alexandru avea o echipă, pe

care am numi-o, astăzi, de experţi în relaţii publice, pe care a luat-o cu el în timpul războiului. Editorii antici au compus scrisori despre război, pentru oraşele din Grecia. În aceste „scrisori personale de pe front ale generalului Alexandru”, ei prezentau totul într-o lumină favorabilă, atunci când veştile erau proaste (precum răniri grave în timpul luptelor victorioase ori nevoia de întăriri). Scrisorile erau adesea însoţite de o parte din prada pe care Alexandru o captura de la persanii mai înstăriţi. Furnizarea unor astfel de scrisori a dat roade. Campania lui Alexandru împotriva persanilor s-a desfăşurat ani la rând, iar grecii au continuat să îl susţină. Nu au existat revolte în Grecia câtă vreme Alexandru s-a aflat în Persia, cu toate că mulţi greci erau încă nemulţumiţi că sunt conduşi de un macedonean. De asemenea, Alexandru a luat în campaniile sale o echipă de istorici, motiv pentru care ştim azi atât de multe despre cea ce a făcut şi despre motivele sale. Istoricii săi au descris în mare parte cu destulă acurateţe şi corectitudine operaţiunile militare greceşti, iar acest lucru ne oferă materiale valoroase, pe care le putem studia prin comparaţie cu războaiele din vremea noastră. Ele ilustrează, totodată, paşii care au fost făcuţi în evoluţia războiului informaţional şi care pot fi recunoscuţi mai ales în operaţiunile cibernetice.

Toţi comandanţii de succes din Antichitate nu numai că s-au bazat pe această strategie, dar au şi conceput reţeaua care distribuia informaţia. Alexandru cel Mare era cunoscut pentru faptul că dorea să afle cât mai multe informaţii posibile despre oponentul său. El nu dorea să ştie numai lucrurile obişnuite (de unde era mobilizată armata inamică, din cine era compusă şi cine o conducea). El căuta detalii suplimentare, precum gradul de loialitate (faţă de împărat) al diverselor provincii prin care el şi armata sa trebuiau să treacă înainte de a începe lupta. Alexandru dorea să ştie cum era clima în ţinutul pe care îl invada şi ce fel de recolte existau. Era capabil să se

folosească eficient de aceste Informaţii. Oricine atacă sau se apără pe internet trebuie să facă acelaşi lucru. Cu cât ştii mai multe despre ceea ce trebuie să înfrunţi, cu atât vei ivea mai mult succes. În timpul campaniilor persane, Alexandru a câştigat războiul informaţional – şi nu a fost doar o chestiune de noroc.

Secole la rând, persanii i-au privit pe greci mai degrabă ca pe o bătaie de cap, nu ca pe o ameninţare majoră. În timp ce Alexandru a adunat cantităţi imense de informaţii despre modul de operare al persanilor, aceştia din urmă au rămas, în mare parte, ignoranţi faţă de capacităţile grecilor. Mare greşeală. Asemenea unui războinic modern, Alexandru a ţinut cont de punctele slabe din sistemul de informare persan. Gândiţi-vă la guvernatorii provinciilor şi la oficiali ca la nişte servere pe internet. Se aşteptau ca anumite tipuri de informaţie să ajungă la ei la anumite intervale de timp. Dacă afli care sunt punctele slabe ale unora dintre guvernatorii de provincii sau oficiali, îi poţi compromite. Neutralizează sau preia controlul asupra mai multor provincii şi în cele din urmă vei deţine controlul asupra întregului sistem (Imperiul Persan). Da, Alexandru a trebuit să ducă un anumit număr de lupte şi să asedieze un număr de oraşe. Dar numai câştigarea luptelor nu era de ajuns ca să înfrângă un imperiu precum cel persan. Ceea ce a făcut Alexandru a fost să înţeleagă cum funcţiona sistemul şi să găsească metode de a-l doborî. Asta în vreme ce Imperiul Persan era, practic, o monarhie absolută. De fapt, multe părţi ale imperiului nu vorbeau aceeaşi limbă şi nu aveau acelaşi grad de loialitate faţă de împărat. Guvernatorii provinciilor şi oficialii imperiali aveau grijă mai ales de ei înşişi. Putem spune că Alexandru a fost un mai bun politician decât împăratul persan. Alexandru şi-a folosit armata ca pe un instrument adiacent, pe lângă promisiunile vizând recompense viitoare, şantaj sau orice altceva i-ar fi trecut prin minte. Mulţi alţi cuceritori,

precum Hanibal sau generalii englezi din timpul Războiului de Independenţă al Americii, au câştigat majoritatea bătăliilor, dar au fost înfrânţi în cele din urmă pentru că nu au putut nimici sistemul împotriva căruia luptau. Erau imperii aşa cum e şi internetul, unde, în mare parte, este vorba despre software, nu despre hardware. Găseşte un mod de a înfrânge sistemul şi inamicul va rămâne, ca să spun aşa, holbându-se la un mesaj de eroare pe ecranul computerului. Alexandru a înţeles tainele sistemului mai bine decât adversarii săi. De exemplu, o numeroasă flotă persană din estul Mediteranei periclita abilitatea lui Alexandru de a obţine provizii şi întăriri din Grecia. Alexandru nu putea cumpăra sau construi o flotă pe măsura celei persane, dar a înţeles că persanii depindeau de un mic număr de porturi fortificate pentru a asigura funcţionarea flotei (hrană pentru miile de soldaţi, docuri pentru repararea navelor, adăpost pentru a scăpa de furtuni). Alexandru s-a axat pe cucerirea porturilor care puteau oferi aceste facilităţi şi flota persană s-a predat pentru că accesul de care avea nevoie fusese blocat. Diplomaţia împotriva guvernatorilor de provincii sau a oficialilor împăraţilor persani a arătat, de asemenea, modul în care a folosit campaniile de informare împotriva duşmanului. De multe ori se spune că Imperiul Persan a fost înfrânt din cauza campaniilor militare ale lui Alexandru, dar nu este adevărat. Alexandru a dezbinat imperiul bucată cu bucată. În locul lui, a creat un sistem mai bun. Alexandru cel Mare „a spart sistemul” existent din Afganistan până în Egipt şi întreaga regiune nu a mai fost niciodată la fel.

Conceptul de „spargere a unui sistem” este o invenţie a secolului XX. Procedeul este antic, dar teoretizarea lui este nouă. Nu e atât de ciudat pe cât sună. Întreaga idee de probabilitate a evoluat de abia în ultimele câteva secole. Totuşi, Alexandru cel Mare a fost din nou cu un pas înainte în privinţa analizelor statistice, care, propriu-zis, au

fost o descoperire a secolului al XIX-lea. Alexandru cel Mare, asemenea multor personalităţi de succes ale Antichităţii, avea capacităţi (precum aproximarea şanselor) bine dezvoltate, dar nimeni de la vremea respectivă nu putea să-şi explice acest lucru. El era, totodată, un lider. Provenea dintr-o familie care dăduse naştere unor personalităţi deosebite de-a lungul mai multor generaţii. Beneficia de pe urma genelor bune.

De asemenea, era inteligent, atletic şi chipeş. Tatăl său crezuse în educaţie în timpul epocii de aur a dezvoltării intelectuale greceşti, care, surprinzător, nu era universal preţuită la vremea respectivă. Deci, Alexandru i-a avut ca profesori pe unii dintre cei mai consacraţi oameni de ştiinţă şi gânditori din acea perioadă. Trebuia, totodată, să dovedească faptul că este demn să moştenească regatul tatălui său, pentru că în vremurile acelea nu exista conceptul de drept divin asupra coroanei; Alexandru trebuia să concureze şi să se afirme. A reuşit şi, de atunci, realizările sale au fost considerate uluitoare. Dar de abia în secolul XX am început să înţelegem mai exact ce a făcut. Printre altele, şi-a construit propria reţea de informaţii şi a distrus-o pe cea a duşmanului.

Nu numai că a fost admirat de oamenii timpului său, dar cei cu deprinderi excepţionale au preluat o parte din tehnicile sale. Două secole mai târziu, politicianul roman Iulius Cezar a folosit tehnicile lui Mexandru cel Mare pentru a prelua conducerea Imperiului Roman. Cezar a înţeles secretele care stau în spatele puterii informaţiei. Istoricul campaniilor pe care le-a dus în Galia (Franţa de azi, Belgia şi zonele adiacente) a fost atât de bine scris, încât, timp de secole, a fost considerat mărturia de netăgăduit a creării Franţei unite, una care nu era în întregime germanică sau celtică.

În timp, s-a înţeles că motivul principal pentru care Cezar a scris toate acele scrisori către Roma, despre campaniile sale (pentru includerea lor într-o carte), a fost

îmbunătăţirea imaginii politice. Într-adevăr, Cezar, la fel ca Alexandru cel Mare, fost extrem de priceput în utilizarea şi controlarea informaţiei. Cezar a fost, de fapt, un maestru al cuvintelor, talent pe care l-a folosit pentru a prelua controlul asupra întregului Imperiu Roman (şi pentru a determina decesul republicii romane). Asemenea lui Alexandru, Cezar a ştiut cum să-şi creeze o imagine bună în vreme ce îşi înfrunta opozanţii. Faptele glorioase ale celor doi lideri politici şi militari au căpătat mai mult sens atunci când, în secolul XX, a fost dezvoltat conceptul de analiza a sistemelor.

Aceste două figuri antice şi-au dat seama cum să dezintegreze sistemele în care trăiau. Azi, ni se pare ceva normal ca mulţi să poată dezintegra porţiuni din internet. Şi asta pentru că ne imaginăm că este firesc ca sistemele să existe şi să fie vulnerabile.

Dar toate aceste lucruri despre sisteme şi distrugerea lor nu sunt noi. Ele există de mii de ani.

HANUL RĂZBOINICILOR INFORMAŢIONALI

Poate că cel mai spectaculos „război informaţional” a fost Temujin (Genghis Han), creatorul Imperiului Mongol. Mongolii au cucerit teritorii din Ungaria până în China, din Rusia până în Orientul Mijlociu. Acest lucru a fost înfăptuit prin folosirea abilă a comunicaţiilor. Genghis Han a adunat informaţii (secrete) cu intenţia de a le furniza comandanţilor care aveau nevoie de ele cât mai repede cu putinţă. A folosit iscoade, dar ceea ce a schimbat regulile valabile pentru secolul al XII-lea a fost implementarea de efect a comunicaţiilor de lungă distanţă. Era ceva similar cu American Pony Express din secolul al XIX-lea, întrucât şi mongolii foloseau călăreţi pentru a transporta corespondenţa la mii de mile depărtare. Mongolii au stabilit staţii de poştă la intervale de 25 – 50 de mile. Călătorii care deţineau o „tăbliţă de autoritate” (un bilet de trecere oficial sub forma unei

bucăţi mici de lemn) puteau lua cai odihniţi şi provizii de la acele staţii. Dacă sunau dintr-un corn înainte de a ajunge la următoarea staţie, erau aşteptaţi cu un cal gata pregătit. Un astfel de călăreţ putea parcurge mai mult de 200 de mile pe zi, iar folosirea curierilor proaspăt odihniţi (existau unii de serviciu la fiecare staţie) permitea ca scrisorile importante să ajungă chiar şi la 400 de mile depărtare într-o singură zi. Acest sistem le facilita generalilor mongoli controlul asupra trupelor pe o distanţă imensă. De asemenea, un astfel de sistem îi permitea lui Genghis Han să organizeze rapid o campanie folosind forţe numeroase, întrucât noi staţii de poştă puteau fi repede stabilite. La vremea respectivă, majoritatea conducătorilor depindeau de spionii şi călătorii din zonele învecinate pentru a obţine avertismente despre posibilele atacuri inamice. Armatele ceva mai bine organizate foloseau un sistem de turnuri, adică o operaţiune *pony express* mai înceată, dat Genghis Han putea organiza o campanie de amploare cu mult înainte ca victima vizată să audă despre ea. Slobozirea armelor asupra duşmanului luat pe nepregătite era încă un avantaj pentru mongoli. În mod normal, unui conducător local i-ar fi luat săptămâni să pună la punct trupele adunate de pe la ferme şi din oraşe. Atunci când mongolii atacau fără avertisment, armatele din defensivă erau tăiate în bucăţi înainte că se poate organiza într-o armată cu adevărat puternică. Astfel, viteza mongolă a multiplicat efectul armelor şi aceasta este prima mărturie din istorie a impactului semnificativ pe care îl are viteza. Este esenţa unui atac pe internet. Cu cât ai mai multă viteză, cu atât este mai slabă apărarea.

EDUARD, SPECIALISTUL ÎN COMUNICAŢII

La scurtă vreme după moartea lui Genghis Han, într-o cu totul altă parte a lumii, Eduard al III-lea al Angliei a preluat tronul. Într-o perioadă în care nu exista tiparul sau mass-media electronică, era dificil să foloseşti tehnicile de

propagandă modernă (precum publicitatea în masă prin ziare, radio, TV). Cu toate acestea, Eduard a reuşit, de-a lungul domniei sale, să creeze o campanie de relaţii publice. Principalul sau instrument erau anunţurile oficiale. Era un procedeu medieval obişnuit, care se folosea, de obicei, ca mijloc pentru proclamarea noilor legi şi regulamente. Anunţurile erau transmise oamenilor prin lecturări publice la târguri, în pieţele oraşelor şi la alte manifestaţii publice. Eduard folosea aceste anunţuri fie şi numai pentru a raporta generalităţi şi a transmite ştiri despre cum se desfăşura Războiul de 100 de Ani din Franţa. Acestea erau scrise, în mod intenţionat, într-un limbaj simplu, pe care oamenii de rând să îl poată înţelege. Eduard îşi declara succesele, nemulţumirile şi controversele cu francezii. Această versiune medievală (secolul al XIV-lea) a CNN-ului, plus toată prada pe care soldaţii englezi au adus-o în Franţa, a creat un entuziasm incredibil pentru război. Propaganda eficientă nu a fost singurul instrument de relaţionare folosit de Eduard. El a avut şi avantajul unui guvern mult mai eficient, care, la rândul lui, se baza pe relaţionare.

Acest lucru s-a întâmplat pentru că normanzii (vikingi stabiliţi în Franţa şi vorbitori de franceză) cuceriseră Anglia în 1066. Vikingii erau un popor extrem de întreprinzător şi susţineau ideea de organizaţie eficientă. Au luat legile din Anglia – care la vremea aceea aplica, asemenea celor mai multe regate europene, o fărâmă din legile şi practicile guvernamentale ale romanilor, germanilor şi celţilor – şi le-au pus în ordine. Franţa a rămas, pe de altă parte, greoaie şi ineficientă, dar asta şi pentru că suprafaţa sa întinsă crea mai multe probleme de guvernare. De aceea, până în anul 1337, când Eduard a fost înfrânt în Războiul de 100 de Ani, el reuşise deja să adapteze toate sistemele existente în Anglia şi să lucreze într-un mediu relativ propice pentru a face afaceri.

A folosit un singur sistem juridic pentru toată

naţiunea, un parlament, un sistem eficient de taxe şi o armată profesionistă plătită. De asemenea, deţinea un sistem de informaţii mai rapid decât avea regele Franţei şi instrumente mai bune pentru a le obţine. Când Eduard al III-lea a plecat la război peste Canal, Franţa avea zeci de sisteme juridice diferite, mai multe parlamente (niciunul la fel de util precum al Angliei) şi o grămadă de îndatoriri şi responsabilităţi pentru lorzii feudali. Eduard a putut dezbina şi cuceri Franţa întorcându-i pe nobili unul împotriva celuilalt. Mai mult decât atât, englezii puteau instrui mai multe trupe, mult mai repede decât francezii (care depindeau de îndeplinirea obligaţiilor feudale, nu de soldaţii care să slujească în baza unui contract). Eduard al III-lea ar recunoaşte internetul drept ceea ce este, un instrument foarte eficient de comunicare şi conducere. I-ar aprecia pe cyber-războinicii de azi, pentru că el ducea lupta lor înainte ca acest termen să fie inventat. Din moment ce oamenii nu creaseră pe atunci instrumentele actuale de analiză a sistemelor şi de transformare rapidă a lor, oricine ar fi fost cel care a adoptat un mod cu desăvârşire nou de a face prima dată aceste lucruri a avut un avantaj imens. Pe atunci, tradiţia avea o mult mai mare influenţă decât are acum. Iniţiativa nu era bine primită şi multe lucruri se făceau la fel an după an, din simplul motiv că aşa fuseseră făcute şi până atunci. Întrucât englezii i-au nimicit pe francezi în timpul Războiului de 100 de Ani, deceniu după deceniu, unii lideri francezi şi-au dat seama că jocul se desfăşura după reguli noi, iar ei nu ţineau pasul. Unii dintre liderii francezi cu iniţiativă au adoptat tehnicile militare superioare ale englezilor (precum armata profesionistă plătită), dar de abia în secolul al XV-lea şi-au dat seama regii francezi că este nevoie de o reformă serioasă. În acel moment, englezii nu au mai putut face ce voiau în Franţa şi războiul a luat sfârşit.

RĂZBOIUL ELECTRIC

Un motiv pentru care europenii (şi colonia lor, viitoarea naţiune purtând numele de Statele Unite ale Americii) au devenit o putere importantă din punct de vedere industrial, economic, intelectual şi militar a planetei este acela că mai mulţi oameni au adoptat ideea nonconformistă conform căreia sistemele ar trebui să se schimbe. În cele mai multe părţi ale lumii, schimbarea era privită ca fiind puţin probabilă şi greşită. China a fost cel mai bun exemplu de stagnare din cauza aderenţei rigide la tradiţie şi a rezistenţei în faţa inovaţiei. Schimbarea a determinat Revoluţia Industrială din secolul al XIX-lea şi Revoluţia Informaţională (din care face parte şi internetul) din secolul XX. Conform standardelor istorice, saltul de la comunicarea prin semnale de fum la internet a fost unul rapid. A durat mai puţin de două secole de la începutul Revoluţiei Industriale până la epoca internetului.

Până în secolul al XIX-lea, turnurile de semnalizare erau singura modalitate de a construi o reţea de comunicaţii la mare distanţă. Deşi se foloseau oglinzi sau steaguri în cele mai multe zone, facilitând transmiterea unui număr mai mare de informaţii în reţeaua de comunicaţii, acestea nu circulau mai repede decât o făceau în urmă cu două mii de ani. În această etapă a dezvoltării tehnicii, chiar şi oamenii de afaceri foloseau aceste reţele. Dar apoi a apărut prima reţea electronică de comunicare, la mijlocul secolului al XIX-lea. Telegraful a reprezentat o revoluţie majoră în comunicaţii, la aceeaşi scară ca şi internetul. Nici măcar telefonul nu a avut acelaşi impact pe care 1 a avut telegraful în 1840. De fapt, telefonul (1870) a fost, practic, o versiune mai scumpă şi, timp de mai multe decenii, numai afaceriştii, oamenii înstăriţi şi guvernele şi l-au putut permite. Dar telegraful reprezenta comunicarea în masă, fiind suficient de ieftin pentru ca toată lumea să îl poată folosi, cel puţin în caz de urgenţe. Guvernul şi mediul de afaceri se foloseau cel mai mult de el şi iată care este momentul în care cyber-războiul a

început să prindă contur; telegraful a început să fie folosit pentru spionaj în vreme de război. Tastarea mesajelor la telegraf a devenit parte din instructajul pentru misiune primit de patrulele de cavalerie infiltrate în liniile inamice. Pentru cei cu înclinaţii matematice, elaborarea şi spargerea codurilor secrete au devenit un fel de hobby; iar atunci când vorbim despre război, adevărul este că cifrurile din secolul al XIX-lea nu erau atât de greu de spart.

În urmă cu un secol, a fost inventat telegraful wireless. La acesta nu mai puteai tăia firele, dar era mult mai uşor de interceptat. De abia în secolul XX, guvernele au luat în serios crearea unor coduri secrete care să fie mult mai greu de descifrat. Dar se pare că nu suficient de greu, întrucât SUA şi Marea Britanie au spart codurile germane şi japoneze în timpul celui de al Doilea Război Mondial. Reţelele electronice de comunicaţii au, în prezent, peste 150 de ani. Prima a fost reţeaua de telegraf. Aceasta nu putea fi folosită în mod direct decât de operatori instruiţi (numiţi chiar „operatori de telegraf”) care cunoşteau atât codul Morse, cât şi cum să folosească echipamentul. Aproximativ patru decenii mai târziu, au început să apară primele reţele de telefonie. Deşi oricine putea fi utilizator, cererile de conexiune trebuiau să treacă pe la operatori. Abonaţii companiilor de telefonie locală îi sunau pe operatori, pentru a fi puşi în legătură cu alţi abonaţi. La vremea respectivă, acest pas în evoluţia tehnicii era considerat la fel de uimitor cum sunt reţelele de calculatoare azi. De abia în anul 1878 a fost deschis primul comutator de telefoane locale (în New Haven, Connecticut), la doi după ce a fost făcută prima demonstraţie cu un telefon.

A durat numai cinci ani până când oraşele aflate la distanţă au început să fie conectate. Pe acea vreme încă mai era nevoie de un operator pentru a pune în legătură abonaţii de la capătul a două telefoane aflate la depărtare.

De exemplu, în 1883, primele apeluri la distanţă au avut loc între New York şi Chicago. În 1884, a fost creată o reţea care lega New York de Boston. În 1915, a fost creată prima reţea telefonică transcontinentală, între New York şi San Francisco. Primul apel transoceanic a fost făcut în 1926, între New York şi Londra. De abia la sfârşitul secolului s-a renunţat la sistemul „sună operatorul, solicită apelul”. De fapt, ultimul schimb de apeluri de acest fel s-a făcut până în 1983 în SUA. înseşi companiile de telefonie nu au devenit suficient de automatizate pentru a permite apelurile la distanţă fără a fi nevoie de asistenţa unui operator (apelarea directă) până în 1951.

De abia în ultimele patru decenii au fost computerizate toate sistemele de telefonie. Înainte de asta, erai nevoit să iei legătura cu mai mulţi oameni înainte de a vorbi cu cineva care se afla la depărtare. Odată ce computerele au preluat controlul, acest lucru s-a schimbat rapid. Dar atunci s-a descoperit că programele de calculator pot fi păcălite mult mai uşor decât ar fi putut fi operatorii umani. Desigur că au existat întotdeauna oameni care au încercat să atragă asupra operatorilor umani diferite acuze şi neplăceri, dar era nevoie de sisteme automate înainte ca primii hackeri autentici să intre în acţiune.

La început, hackerii nu foloseau PC-uri pentru a ataca reţeaua telefonică; PC-urile nu fuseseră încă inventate şi era dificil să obţii acces la computerele folosite de către compania telefonică. Mai degrabă, acei „spărgători de telefoane” ai anilor ’60 foloseau aparate manuale, pe baterie, care emiteau diferite sunete electronice către telefonul companiei care controla reţeaua de apeluri la distanţă. Chiar dacă unii dintre aceşti spărgători puteau fluiera acele sunete, oricine putea folosi acele cutii electronice. Singurul lucru pe care îl puteau obţine era să efectueze apeluri la mare distanţă pe gratis. Dar chiar şi aşa, era suficient pentru a atrage o mulţime de

oameni către această practică. Lupta dintre companiile de telefonie şi spărgătorii lor se duce şi în zilele noastre, chiar dacă atenţia este îndreptată, în cea mai mare măsură, către atacatorii sistemelor telefonice echipaţi cu computere personale.

Reţelele telefonice vechi de un secol au devenit apoi subiectul altor forme de cyber-război, în special prin monitorizarea convorbirilor. Aceasta era folosită legal şi ilegal pentru obţinerea unor avantaje în probleme comerciale şi militare. De asemenea, telefoanele erau folosite pentru a trimite informaţii eronate. Era mai uşor să imiţi vocea cuiva decât să te deghizezi în acea persoană. Dar reţeaua telefonică în sine prezenta siguranţă. Utilizatorii telefoanelor nu puteau pătrunde în software-ul care administra uriaşele reţele telefonice.

ORIGINILE PROBLEMELOR NOASTRE ŞI ALE WORLD WIDE WEB

Apariţia World Wide Web (sau „webul”, „internetul”, „netul”) nu a fost planificată. A venit din trei direcţii diferite, într-un mod destul de imprevizibil. Este o poveste ciudată, dar adevărată.

La început au apărut computerele multifuncţionale, care au fost create la începutul anilor ’60. Era o evoluţie naturală a computerelor extrem de scumpe din perioada respectivă (conform standardelor de atunci). Era foarte scump să deţii vreunul din aceşti monştri de mai multe milioane de dolari, chir dacă era nou-nouţ. La sfârşitul anilor ’50, cercetătorii au venit cu un plan de a face aceste sisteme multifuncţionale să funcţioneze şi până la începutul anilor ’60 ele puteau rula mai mult de un singur program în acelaşi timp. Nu a durat mult până când au apărut programe care permiteau schimbul de mesaje-text şi chiar discuţii în timp real între diferiţi utilizatori de la diferite terminale. Totuşi, nu puteau fi folosite decât de grupuri de oameni care utilizau acelaşi computer. Nu

exista vreo problemă cyber-războinică în acest stadiu, iar în acea perioadă au apărut e-mailul şi mesajele în timp real, chiar şi numai între oameni care foloseau acelaşi calculator.

În anii ’60 a devenit foarte populară ideea de a conecta computerele la telefon. Modemurile existau încă din 1955. Primele astfel de aparate au fost create pentru a face legătura între sistemele de apărare aeriană ale SUA. Dar aceste prime modemuri erau mari, scumpe şi încete (110 bauzi). Singurii care şi le puteau permite erau oamenii de afaceri. Nicidecum nu era un produs pentru mase. Şi acest lucru nici nu avea cum să se întâmple până când tehnologia nu devenea mai ieftină. Multe dintre cercetările făcute asupra reţelelor de calculator au fost finanţate de guvernul SUA, un proiect care mai târziu a facilitat apariţia internetului. În timpul anilor ’70 au fost dezvoltate reţelele comerciale (între diferite tipuri de afaceri). Au apărut companii precum Tymshare, Compuserve şi Telenet, care au pus în vânzare computerele *mainframe* ce furnizau o gamă largă de software pentru afaceri şi acces la baze de date. Acestea erau supravegheate de profesionişti, iar dacă ar fi existat vreo problemă, ea ar fi venit din interior. Aceste sisteme nu erau nici pe departe atât de uşor de spart precum este internetul. Încă nu exista vreo ameninţare de cyber-război.

Dar la sfârşitul anilor ’70, jocul a început să devină interesant. Ceea ce urma să se întâmple era complet neaşteptat. De fapt, trei sisteme online diferite erau în curs de dezvoltare. Cele evidente erau reţelele comerciale (pentru afaceri) şi ARPANET (un experiment finanţat de guvern pentru a crea un sistem de comunicare robust în cazul apariţiei unui război nuclear). Dar cel de al treilea element era absolut surprinzător: BBS-uri (Bulletin Board Systems) utilizate de persoane individuale.

Cele trei sisteme s-au unit în ceea ce azi numim World Wide Web (versiunea grafică a internetului). Toate

problemele pe care le avem cu securitatea internetului şi cyber-războiul au izvorât din modul în care aceste trei concepte diferite ale lumii online ar trebui să fuzioneze.

La urma urmei, internetul a fost creat bucată cu bucată. De exemplu, în anul 1962, AT & T a lansat un modem comercial (câteva mii de dolari pentru 300 de bauzi). Aveai nevoie de modemuri pentru a conecta ieftin calculatorul prin sisteme telefonice. Dar modemurile au rămas scumpe şi încete până când legea a fost schimbată în 1975 şi toată lumea a avut dreptul să se conecteze la sistemul telefonic fără să mai aibă de a face cu o companie de telefonie. Înainte de aceasta, companiile de telefonie făceau ca utilizarea unui modem să fie dificilă şi scumpă. Ca urmare a acestei schimbări şi a introducerii PC-urilor, la sfârşitul anilor ’70, compania Hayes a început să producă, în anul 1977, modemuri mai ieftine şi a stabilit standarde pentru utilizarea lor de către clienţi.

Aceste modemuri s-au vândut foarte bine, dar ele erau achiziţionate în mod special de întreprinderile comerciale care doreau o conexiune mai ieftină la companiile de servicii online costisitoare precum Compuserve.

Apoi, în 1978, primele BBS-uri (Bulletin Board Systems) au fost date în funcţiune. Create de împătimiţii PC-urilor în primul rând pentru a vedea dacă se pot face, această idee simplă a dat naştere la o altă revoluţie. Aceste sisteme foloseau PC-urile pentru a rula un program BBS care permitea altor utilizatori de PC-uri să acceseze BBS-ul cu programe de telecomunicaţii (telecom) pentru a lăsa şi citi mesaje (pe BBS), dar şi pentru a trimite şi primi fişiere (programe, date, imagini cu femei dezbrăcate, orice). Singurul element de care mai lipsea era modemul, care permitea PC-ului să trimită şi să primească date prin linia telefonică. Atunci când au apărut primele modele de modemuri Hayes, la sfârşitul anilor ’70, preţul a scăzut rapid la mai puţin de 500 $. Primele astfel de modemuri

erau destinate proprietarilor de PC-uri. Aceasta este încă o dovadă a impactului imens pe care l-a avut apariţia PC-urilor la sfârşitul anilor ’70. Primele modemuri erau încete (300 de bauzi sau aproximativ 30 – 37 de caractere pe secundă versus 56.000 de bauzi la sfârşitul anilor ’90), dar i-au reunit pe oameni. În numai câţiva ani, mii de BBS-uri erau date în funcţiune, unele dintre cele mai populare având linii telefonice multiple, iar costurile anuale sau lunare pentru utilizarea lor erau reduse. Până în 1990 existau mai mult de 30.000 de BBS-uri, cea mai mare parte dintre ele în SUA. Majoritatea erau un simplu hobby pentru operatori. Acest lucru era în spiritul a ceea ce apăruse printre mulţii împătimiţi sau profesionişti într-ale computerelor, utilizarea în comun a unui serviciu public. Această atitudine avea să fie dusă mai departe pe World Wide Web, întrucât acolo ajung cei mai mulţi dintre operatorii BBS. Dar pe parcursul anilor ’80 şi până la începutul anilor ’90, toate lucrurile ieşite din comun, asociate cu webul (hackingul, entuziasmul utilizatorilor şi chestiile noi), au fost condiţionate de creşterea comunităţii BBS. Exista o singură mare diferenţă, lumea BBS era mult mai mică, iar tehnologia era mai complicată decât ceea ce vedem azi pe internet. Webul este o piaţă de masă, scena BBS se adresa în mare parte tocilarilor sau celor care doreau să se lupte cu sfârşitul dur al tehnologiei computerelor.

Chiar şi pe măsură ce BBS-urile erau create, serviciile de comunicare a datelor comerciale creau, la rândul lor, o altă comunitate online. În 1979, Compuserve, a cărui reţea de afaceri stagna la sfârşitul zilei de lucru, a decis să ofere acces utilizatorilor din timpul nopţii şi în weekend. 12 sau 24 $ pe oră (în funcţie de oră) nu era un preţ mic (20 – 40 $ pe oră în banii de azi), dar a creat o comunitate world wide a celor care nu puteau ajunge acolo unde era guvernul: pe internet. La vremea respectivă, Webul era încă un proiect de cercetare al Departamentului

Apărării (ARPANET). Acest proiect a început în anul 1969 şi până în 1971 era deja dat în folosinţă cu 23 de „noduri”-gazdă pe care le puteai accesa de la universităţile importante. ARPANET nu a trimis primul e-mail până în 1972 şi nu a atins o mie de noduri până în 1984. În timpul anilor ’70 şi 80, reţelele comerciale precum Compuserve erau mult mai puternice. Chiar şi comunitatea BBS era mai mare decât internetul în timpul anilor ’80.

Compuserve a constatat apoi că permiterea accesului în sistemul său a celor din afară în timpul serii a dus la primele incidente a ceea ce azi numim hacking. Utilizatorii puteau crea software-uri, le puteau testa şi rula pe computerele Compuserve. Dar faptul că erau lăsaţi liberi pe aceste calculatoare era prea tentant pentru hackeri încât să joace corect. Aceştia au început imediat să divulge puncte slabe din securitatea Compuserve şi, înainte de a deveni prea dăunători, compania le-a blocat accesul. Cu toate acestea, era un avertisment asupra celor ce urmau să se întâmple.

În timpul anilor ’80, serviciile comerciale precum Compuserve (şi un rival mult mai neînsemnat care mai târziu a devenit AOL) erau ACELE reţele pe care trebuia să fii. În anul în care

Compuserve a trecut online, internetul a introdus compatibilitatea BBS (se numea „grup de ştiri”). Dar oricât de active erau aceste grupuri, „forumurile” de pe Compuserve erau cele unde se petrecea acţiunea. Un motiv era faptul că reţelele comerciale atrăgeau utilizatorii cu o mai bună educaţie. Şi pentru că trebuia să plăteşti pentru acces, hackerii, care întrerupeau discuţiile de grup pe BBS şi internet, erau ţinuţi la distanţă. În acea perioadă, internetul era încă disponibil numai universităţilor şi Departamentului Apărării.

Asta nu înseamnă că un grup de oameni educaţi este format întotdeauna din îngeri. Exista o mare incidenţă de discuţii zgomotoase („flăcări”) pe teme tehnice între

utilizatori. Până în anul 1989, erau numai două milioane de utilizatori online ai serviciilor comerciale, inclusiv aceia (probabil jumătate) care erau utilizatori comerciali ce se bucurau de partea noncomercială a acestor servicii. Numărul total al oamenilor online era de aproximativ cinci milioane. Majoritatea dintre aceştia nu foloseau sisteme comerciale sau internetul în timpul anilor ’80. Nu, majoritatea proprietarilor de modemuri se aflau pe reţele complet neaşteptate, o reţea a Bulletru Board Systems. BBS reprezenta o utilizare surprinzătoare, de la firul ierbii, a PC-urilor, modemurilor şi liniilor telefonice.

Începând din 1978 până în prezent, au existat, la un moment dat, mai mult de 100.000 de BBS-uri. Dar până la începutul anilor ’90, comunitatea BBS şi serviciile comerciale se luptau pentru cota de piaţă. Cu toate că serviciile comerciale erau oarecum mai uşor de utilizat decât BBS-urile, acest lucru avea să se schimbe. Software-ul BBS era creat de mii de programatori independenţi, plini de energie. Era generaţia PC care revoluţiona afacerea cu software. Până în 1990, programele grafice (precum Windows sau MacIntosh) erau în proces de dezvoltare, înlesnind accesul online şi utilizarea a tot ce avea BBS de oferit. Ceea ce atrăgea cel mai mult erau preţul şi simţul comunităţii. Cele mai multe BBS-uri erau gratuite, cu toate că era dificil să poţi ajunge pe unul popular la o oră de vârf. Acest lucru a dat naştere la un nou instrument de hacking, programul de formare automată a numărului de telefon.

Creat pentru a ajuta la conectarea la BBS atunci când toate liniile modemului erau ocupate, programul de autoformare a numărului încerca până când era realizată conectarea. Un alt program care a apărut prima dată pentru utilizatorii BBS a fost cititorul offline. Acest program aduna toate mesajele BBS în aşteptare, le trimitea pe e-mail şi se deconecta. Era considerată o dovadă a bunelor maniere, întrucât permitea mai multor

oameni să se conecteze. Totuşi, cel mai utilizat serviciu BBS era transferul de fişiere. BBS a fost considerat Epoca de Aur a shareware-ului (programe scrise şi distribuite gratuit în ideea că, dacă îţi va plăcea, vei plăti pentru el). Tot în anii ’80 au apărut şi primele scannere ieftine, iar conţinutul foto al revistelor *Playboy, Penthouse* sau *Hustler* a început să fie rapid transferat pe BBS ca fişiere. Cele mai populare transferuri de fişiere (de la BBS către utilizatorul computerului) erau fotografiile cu femei dezbrăcate şi programele shareware.

La mijlocul anilor ’80, sistemele BBS au evoluat în propria versiune de internet sub forma Fido Net, care în momentul lui de vârf (1995) avea peste 50.000 de noduri (mesajele furnizate de BBS de la serverul local). Fido Net s-a remarcat pentru că a apărut pe neaşteptate într-o lume a BBS-urilor individuale. Mulţi operatori de sistem au fost de acord să instaleze software-ul Fido Net, care aduna mesajele BBS, le trimitea pe e-mail, după care erau trimise mai departe, către alte sisteme Fido Net. Într-o singură zi, fiecare BBS Fido Net avea panelul de mesaje al tuturor celorlalţi şi totodată e-mailuri trimise. Fido Net era tipic ideilor şi software-ului create de programatori de la sfârşitul anilor ’70 până la începutul anilor ’90. Înainte de explozia forumurilor pe internet exista o expansiune la fel de mare a subiectelor abordate în grupurile de Fido Net (şi alte sisteme similare). BBS-urile şi sistemele comerciale găzduiau şi ele câte un chat room, înainte ca acestea să devină hit pe internet.

Tipul de extindere a software-ului şi conceptelor internetului de care ne aducem aminte din anii ’90 s-a realizat într-o formă mai primitivă în timpul anilor ’80 în comunitatea BBS. De la apariţia webului, reţeaua Fido Net s-a micşorat (la aproximativ 10.000 BBS-uri, cele mai multe în afara SUA) din cauza popularităţii mai mari de care s-a bucurat internetul.

Între timp, în anii ’80, ARPANET a continuat să

crească şi să evolueze, dar era încă în mare parte un proiect de cercetare finanţat de guvern. Termenul „internet” nici nu a fost măcar inventat până în anul 1982, dar atunci când s-a întâmplat, s-a creat o presiune din ce în ce mai mare pentru a putea fi folosit de toată lumea. Dar de abia în anul 1986 ARPANET a decis să deschidă Webul şi pentru cei care nu erau angajaţi sau contractori ai Departamentului Apărării. Acesta a fost momentul în care internetul cu toate opţiunile disponibile a devenit realitate. Un set standard de protocol electronic a facilitat conectarea la internet a oricărei reţele (ceea ce însemna de fapt internetul, o colecţie de reţele separate care puteau comunica între ele).

ARPANET a fost oprit în 1990, când a fost lansat internetul ca reţea publică. În 1988 fusese introdus Sistemul Nume de Domeniu, care facilita accesul; înainte de aceasta, pentru a ajunge la o pagină de internet era nevoie să tastezi adresa ei numerică (precum 123.456.789.0). Odată cu sistemul serverului Nume de Domeniu, puteai găsi un computer-gazdă cu vechea adresă numerică sau tastând numele acestuia (mydomain.com).

Multe organizaţii au văzut imediat avantajele oferite de internet, pentru că ceea ce făcuse proiectul de cercetare ARPANET era rezolvarea problemelor de comunicare dintre diferite reţele. Nu exista un standard al comunicării computerizate prin telefon, iar organizaţiile erau din ce în ce mai dornice să comunice electronic cu furnizorii şi clienţii. Multele sisteme incompatibile ale calculatoarelor făceau ca acest lucru să fie dificil de realizat. Dar internetul a rezolvat problema. După ce acesta şi-a deschis porţile pentru cei din afară, la sfârşitul anilor ’80, corporaţiile au fost cele care căutau metode de a folosi toată această tehnologie utilă şi gratuită (guvernul nu brevetase internetul). Gratuitatea fusese oferită intenţionat, cu scopul de a aduna cât mai mulţi oameni care să folosească Webul. Între timp, pe la mijlocul anilor

’90, principalii cumpărători ai software-ului BBS erau corporaţiile care foloseau sistemele BBS aşa cum este în prezent folosit internetul la locul de muncă. Deşi internetul era util, iar software-ul lui era gratuit, nu era chiar atât de uşor de folosit.

Dar, de fapt, internetul era o interfaţă a unei linii de comandă (gândeşte-te la DOS, la comenzile necesare pentru a programa computerul să efectueze o operaţiune) intimidantă pentru mulţi potenţiali utilizatori. Acest lucru s-a schimbat între 1989 şi 1993, întrucât a fost creat motorul de căutare. Acesta era o pagină grafică a internetului şi avea acelaşi efect ca înlocuirea DOS-ului cu software-ul Windows. Dintr-odată, internetul era mult mai simplu de folosit. Au fost create din ce în ce mai multe gazde care să fie accesate numai printr-un motor de căutare. După ce a apărut primul motor de căutare gratuit (Mozaic), la sfârşitul anului 1993, numărul utilizatorilor de internet a explodat.

La sfârşitul anului 1988, existau 100.000 de computere-gazdă şi numărul a început să crească după ce guvernul a oferit acces liber la internet mai multor oameni. În 1993, când a fost lansat motorul de căutare, existau 400.000 de computere-gazdă pe internet. Până în 1994, numărul lor a ajuns la 600.000. În 1995 erau un milion, iar în 1996, un milion şapte sute. În următorii ani s-a înregistrat o creştere explozivă. La sfârşitul anului 2001 erau 12 milioane de servere web active. Mai mult de un miliard de pagini web erau disponibile pe internet şi existau 400 de milioane de utilizatori în lume (135 de milioane numai în SUA). Numărul utilizatorilor online din SUA a crescut de la 6% în 1993 la 42% în 2001. În acel an, aproximativ o treime din creşterea economică a SUA a fost posibilă, în mod direct sau indirect, prin internet.

În acelaşi timp, s-au întâmplat şi lucruri care au favorizat această creştere explozivă. Cel mai important a fost accesul la modemuri mai ieftine şi mai rapide. În 1989,

existau aproximativ şapte milioane de modemuri, şi asta după 12 ani în care companiile comercializaseră modemuri mai ieftine şi mai rapide. Dar în anii ’90, viteza standard a unui modem a urcat de la 9.600 de bauzi la 56.000 de bauzi. Preţul unui modem a scăzut până la sub 50 $, iar vânzările au depăşit 50 de milioane de modemuri pe an. În 1993, SUA aveau 12, 6 milioane de utilizatori de modemuri, iar în următorul an, 16, 4 milioane. Până în anul 2000, mai mult de jumătate din gospodăriile americane erau online.

Sistemul de operare Windows (3.0) din 1993 a fost de asemenea o lansare importantă pe scena internetului. Acest software Windows a fost comercializat împreună cu majoritatea milioanelor de noi computere cumpărate în fiecare an. Cu Mozaic sau Netscape, care erau şi ele pe motorul de căutare web, tot ceea ce trebuiau să facă utilizatorii era să selecteze simbolul motorului şi erau online. Odată cu programele Windows uşor de utilizat, mult mai mulţi oameni erau dornici să se „joace” pe calculator, iar în momentul în care accesau webul prin motorul de căutare, deveneau dependenţi.

La sfârşitul anului 1994, Netscape Corporation a lansat primul motor de căutare comercial. Putea fi obţinut prin descărcare gratuită, dar numai 5% din cei care foloseau iniţial Netscape l-au descărcat (cu toate că era foarte mediatizat). Cei mai mulţi îl obţineau împreună cu noul computer, iar Netscape a făcut acest lucru posibil prin înţelegerile încheiate rapid cu toţi marii producători de calculatoare. Producătorii erau mai mult decât bucuroşi să facă acest lucru, întrucât era evident că Mozaic avea un succes enorm şi că Netscape reuşise să creeze un motor de căutare şi mai bun.

O altă schimbare majoră adusă de web a fost că utilizatorii nu mai erau, în cea mai mare parte, elevi şi studenţi. La sfârşitul anului 1995, 3, 3 milioane de oameni se conectau la internet printr-un server aflat într-o

universitate. Drept urmare, 6% dintre americani cu vârsta cuprinsă între 18 şi 29 de ani foloseau World Wide Web, dar numai 1 % aveau peste 50. În timp ce 8% dintre americanii cu studii superioare foloseau World Wide Web, numai 1% dintre cei cu studii liceale o făceau. În 2001, caracteristicile utilizatorului mediu de web erau mult mai apropiate de demografia populaţiei în general.

Pe măsură ce anii ’90 deveneau istorie, calculatoarele au devenit mai ieftine, webul a crescut şi erau tot mai multe lucruri pe care le puteai face cu un motor de căutare. Utilizarea BBS-ului a scăzut odată ce utilizatorii au aflat că pot face aceleaşi lucruri mult mai uşor pe web. BBS-urile înseşi au devenit fie ISP-uri (Internet Service Providers, care furnizau internet utilizatorilor BBS), fie au dispărut. Mulţi dintre operatorii de sistem BBS erau bucuroşi să creeze site-uri web, care făceau acelaşi lucru ca BBS-urile, dar cu mult mai puţină bătaie de cap. Mai mult decât atât, un site web le oferea operatorilor de sistem un public mult mai mare. Dar acest lucru nu aducea numai avantaje, întrucât comunităţile BBS erau, de cele mai multe ori, locale şi formau bisericuţe (chiar dacă rareori se întâlneau faţă în faţă). Dar pe web, întâmplător şi adesea abuziv, personaje diferite puteau să vină şi de multe ori chiar veneau. Cheltuielile erau mult mai mici, iar experienţa BBS oferea utilizatorilor un început cu dreptul către ocazii de neratat în explozia dot.com. În general, operatorii de sistem s-au descurcat foarte bine.

Serviciile comerciale fie s-au transformat în ISP-uri, fie au dat faliment. AOL a fost conectat la internet în 1994, cu toate că folosea internetul de câţiva ani pentru transferul de e-mailuri. Conexiunea de e-mail a fost de fapt impusă serviciilor comerciale de clienţii corporatişti, care într-un fel sau altul le-au spus să obţină acest tip de interconectivitate (altfel corporaţiile o vor face singure şi poate nu aveau nevoie de toate acele mii de conturi

comerciale de utilizatori). Multe organizaţii foloseau deja reţele comerciale şi tehnologia BBS, dar şi-au dat seama că este mult mai uşor de navigat pe internet cu ajutorul unui motor de căutare.

Cei mai mulţi oameni nu şi-au dat însă seama de faptul că securitatea pe internet nu era nici pe departe la fel de puternică precum era cea a reţelelor comerciale sau chiar a BBS-urilor. Exista o parte întunecată la toate aceste lucruri şi s-a dovedit a fi mult mai întunecată decât s-ar fi aşteptat oricine.

PARTEA ÎNTUNECATĂ

Viruşii informatici nu erau unici pe internet. Au apărut pentru prima dată în perioada de glorie a BBS-ului. Primul virus PC a apărut la începutul anilor ’80 şi a fost conceput drept o glumă sau un mod prin care programatorii să iasă în evidenţă. Viruşii chiar afişau mesaje care le comunicau utilizatorilor că au fost infestaţi. Dar până la mijlocul anilor ’80 au început să apară mai mulţi viruşi dăunători. Aceştia s-au răspândit rapid din cauza milioanelor de fişiere transferate în fiecare zi prin BBS. Deşi mulţi dintre operatorii de sistem erau profesionişti experimentaţi, cei mai mulţi dintre ei nu erau experţi software. Ideea acestor viruşi i-a luat pe operatorii de sistem prin surprindere. Mai rău, numai BBS-urile mai mari şi mai bine încărcate verificau existenţa viruşilor şi acest lucru necesita timp. Pentru că majoritatea BBS-urilor erau create din pasiune, tot ce făceau operatorii de sistem era să posteze un mesaj care avertiza utilizatorii, le spunea oamenilor că sunt pe cont propriu şi să aibă grijă. Internetul era în aceeaşi barcă, cu excepţia câtorva FTP-uri (site-uri de stocare a fişierelor), unde cineva verifica programele încărcate de o posibilă „infestare”. Pe sistemele comerciale au scăpat mai puţini viruşi, pentru că aici existau oameni care verificau programele încărcate înainte să fie puse la dispoziţia publicului.

Până la sfârşitul anilor ’90, internetul a fost efectiv o operaţiune în dezvoltare (mulţi susţin că încă mai este). Natura experimentală a internetului a dus la un progres rapid în rezolvarea unor probleme tehnice şi la crearea a multe alte software-uri. Sistemul era construit în aşa fel încât oricine să poată avea acces la alte computere de pe net. Securitatea era o prioritate de mică importanţă, pentru că aproape toţi cei care lucrau în acest domeniu se cunoşteau între ei (sau ştiau unii de alţii). În plus, rata experţilor în calculatoare în rândul utilizatorilor era foarte ridicată. Oricine ar fi pus la cale acte distructive ar fi fost prins şi ar fi suferit umilinţa de a fi pedepsit de colegii săi.

În anii ’90, internetul devenise o reţea internaţională şi aduna milioane de noi utilizatori în fiecare an. Spiritul energetic şi jucăuş care făcuse ca tehnologia să progreseze atât de rapid se întorsese pentru a bântui spaţiul cibernetic. Mulţi dintre acei hackeri „jucăuşi” au decis că este mai amuzant să distrugă sistemul decât să îl dezvolte şi să îl menţină. Deşi aceia care aveau computere personale conectate la net erau conştienţi de vulnerabilitatea lor, nu toţi îşi actualizau sistemele la fel de des pe cât ar fi trebuit pentru a ţine intruşii la distanţa. Mai mult, exista întrebarea dacă internetul poate fi gândit ca un spaţiu sigur.

Internetul a fost dezvoltat ca un proiect organizat cu lejeritate, iar oficialii guvernului SUA care l-au finanţat, au încurajat ideea de a crea un net „lejer”. Asta înseamnă că dacă părţi mari ale internetului ar fi fost lovite de să zicem, un război nuclear, elementele supravieţuitoare ar putea funcţiona în continuare. Deşi guvernul nu a păstrat tăcerea asupra aspectului „supravieţuirii războiului nuclear” pe internet, nici nu l-au scos în evidenţă. Cei care construiau internetul, mulţi dintre ei voluntar, au văzut şi avantajul unei reţele care să nu fie controlată de o autoritate centrală. Era ca un roi de albine. Puteau ucide părţi din el, dar nu pe tot. Conceptul tradiţional al unei reţele era ca un

elefant defilând, caz în care un singur glonţ, suficient de mare şi tras în locul potrivit, ar fi distrus întregul spectacol.

Internetul înseamnă milioane de computere individuale, unite prin linii telefonice, software-uri comune şi destinate pentru transferul informaţiilor. Un computer conectat la internet poate fi un sistem desktop folosit de o persoană sau un *mainframe* împărţit între mii de utilizatori.

Fiecare computer (sau grup de computere) de pe internet are propria adresă, precum BROWN.EDU pentru o universitate, ARMY.MIL pentru armata SUA, MOBIL.COM pentru o corporaţie sau AOL.COM pentru o mare reţea comercială. Deşi toate aceste computere folosesc software comun pentru a facilita schimbul de informaţii, ele folosesc mii de sisteme de operare diferite pe aparatele individuale.

Cu toate acestea, în anii ’90, internetul a devenit atât de mare şi de complex, încât nimeni nu mai înţelegea cu adevărat întregul sistem. Nu se ştia cu siguranţă care erau toate lucrurile mârşave pe care le puteai face diferitelor tipuri de calculatoare conectate la internet. Unele dintre aceste computere erau mai vulnerabile decât altele. Tot ce trebuia să faci era să te strecori într-un calculator conectat la internet şi acest lucru divulga adesea parole şi alte informaţii care îţi facilitau accesul la multe alte sisteme. Drept urmare, multe companii au început să creeze pentru ele sau pentru comercializare software-uri firewall care izolau un calculator conectat la internet de celelalte din sistem. Dar pentru că aproape orice tip de computer (de la PC la *mainframe)* putea fi conectat la internet, nu toate sistemele firewall erau la fel şi nici nu erau la fel de eficiente.

Pentru ca lucrurile să devină şi mai complicate, reţelele locale (LAN-urile) au început să fie folosite mai mult în timpul anilor ’70. Aşa cum sugerează şi numele, LAN-urile sunt computere din aceeaşi clădire legate între

ele prin cabluri. Când unul dintre computerele dintr-un LAN era conectat la internet, la fel erau şi celelalte aparate din reţea şi, de obicei, oricine de pe internet putea ajunge la ele. Reţelele existente înainte erau controlate de profesionişti şi prezentau o mai mare siguranţă. Dar LAN-urile erau simplu de instalat şi de folosit de către clienţii-ţintă, utilizatori de tehnologie mai puţin avansaţi. Din păcate, aceştia nu puteau face faţă problemelor de securitate şi acest lucru a transformat reţelele LAN în terenul de joacă preferat pentru vandalii de pe net.

În 1988 a lovit primul vierme major de pe internet. Este vorba despre Morris, care a afectat 10% din cele 60.000 de computere-gazdă conectate în acea perioadă la internet. Asemenea primilor viruşi de PC, viermele nu fusese creat cu intenţia de a provoca prea multe pagube. Domnul Morris se infiltra în sistem şi încerca să creeze un program care că se poate răspândi pe web şi să conducă în secret cât mai multe computere cu putinţă. Era un exemplu tipic de hacking. Nimeni nu acorda permisiunea şi nu supraveghea activitatea. Autorul avea un motiv îndreptăţit (deşi periculos şi foarte criticat) pentru a crea viermele: distribuirea software-urilor şi a actualizărilor. Dar viermele conţinea nişte erori, o simplă întâmplare. Este greu să testezi un virus sau un vierme al internetului fără a-l răspândi în întreaga reţea. Erorile viermelui Morris au făcut ca acesta să se înmulţească pe computerul pe care îl ataca, blocând toată activitatea calculatorului. Din fericire, viermele nu funcţiona decât pe aparate cu anumite configuraţii de hardware şi software, dar tot a reuşit să se răspândească pe mai multe computere prin intermediul netului.

Cu toate că viermele Morris a fost un eveniment media, el a mai fost remarcabil şi din alte motive. Existau date despre viermi încă de la începutul anilor ’80, din care s-a şi inspirat Robert T. Morris. Însă el nu a acordat suficientă atenţie incidentelor anterioare legate de viermii

slab elaboraţi care circulau printre LAN-uri. În general, viermii erau creaţi cu intenţii bune, precum actualizarea software-ului, punerea în funcţiune a calculatoarelor nefolosite pe timpul nopţii sau distribuirea informaţiilor urgente. Până la Morris, nimeni nu se gândise să atace webul cu un vierme. Troienii răspândiţi prin programele infestate postate pe BBS erau înceţi, fiind nevoie de ceva timp pentru a se răspândi. Viermii foloseau software de internet încorporat pentru a ajunge în serverele care foloseau acelaşi tip de software. Da, internetul era mai eficient decât BBS-ul şi reţelele comerciale, dar acum revoluţia electronică se îndrepta către parte întunecată. De fapt, Morris nu a intenţionat să atace internetul, ci a făcut acest lucru din greşeală. Însă, ca urmare a acestei greşeli, internetul a dus la formarea CERT (Computer Emergency Response Team) şi a altor câteva organizaţii care să studieze securitatea internetului şi să furnizeze suport eficient şi rapid în cazul în care ceva asemănător viermelui Morris ar mai avea loc în viitor. Ceea ce, desigur, s-a întâmplat. De aceea, următorul pas a fost convingerea că rezolvarea erorilor de software va îndepărta problemele de la sine. Dar natura software-ului web făcea ca toate software-urile noi să aducă cu de noi erori pe care hackerii să le exploateze. Această problemă pare fără sfârşit. Ce s-a întâmplat cu domnul Morris, omul care a iniţiat acest cerc vicios? A fost condamnat, amendat, pus într-o perioadă de probă de trei ani, după care a devenit un milionar dot.com.

Şi reţelele de telefonie au suferit schimbări. În primul rând, ele transferă mult mai multe informaţii în prezent, chiar în mai multe moduri. Sateliţii şi transmiţătorii prin microunde transportă un trafic foarte mare, la fel şi date. Din ce în ce mai des, mesajele sunt roboţi care vorbesc cu alţi roboţi. Da, roboţi. Timp de mai bine de jumătate de secol, percepţia populară a robotului era aceea a unei maşinării cu formă de om care se poate mişca, vorbi şi într-o anumită măsură poate chiar gândi. În realitate, tot

mai multe lucruri au fost automatizate în ultimele decenii folosind aparatură controlată prin computer. „Roboţii” se găsesc de obicei în cutii de metal, mari şi mici, adesea blocaţi în camere mici sau dulapuri. Aceste „maşini gânditoare” controlează energia, comunicaţiile şi o serie de activităţi din fabrici şi de oriunde în altă parte unde se execută activităţi simple şi repetitive. Deşi aceste funcţii pe care le îndeplinesc sunt simple şi repetitive, ele sunt de multe ori vitale. Dacă unul dintre aceşti roboţi face o greşeală sau este sabotat, alimentarea cu energie dintr-un oraş poate pica, serviciile telefonice de pe o suprafaţă mare pot fi întrerupte sau o bancă poate fi jefuită.

Ceea ce armata numeşte „războiul informaţional” se derulează la un nivel mai înalt de când roboţii au preluat o mare parte din munca de rutină. Dar oricât ar fi de muncitori, eficienţi şi mereu mulţumiţi, aceşti roboţi nu sunt foarte inteligenţi. Dacă un om poate intra în contact cu ei, acesta îi întrece de multe ori în ceea ce priveşte luarea deciziilor. Chiar dacă roboţii „poliţişti” sau „gărzi” sunt puşi acolo pentru a proteja robotul „lucrător”, tot omul deţine supremaţia. Cel puţin până acum.

Pentru că este mai uşor de folosit, o mare parte din controlul roboţilor de la distanţă se face pe internet. Acest lucru îi sperie pe oameni, deşi nu ar trebui. Cu toate că multe servicii (energie, salubrizare, comunicaţii) permit accesul de la distanţă către roboţi, nu există o „centrală de control a roboţilor”. Un sabotor ar trebui să caute care sunt site-urile ce controlează roboţii, să îşi dea seama cum să pătrundă pe ele, după care să provoace pagube la scară largă. Există însă puţine şanse ca acest lucru să se întâmple. Aceste site-uri de control la distanţă se schimbă în permanenţă, astfel încât ceea ce ştii acum despre un site poate fi inutil peste şase luni. Da, internetul este vulnerabil, dar este de asemenea vast şi într-o permanentă schimbare.

Una este să porneşti roboţii telefonici pentru a

efectua apeluri la distanţă şi altceva e să încerci să pui mâna pe câteva milioane de dolari de la sistemele automate de transfer monetar ale băncilor. Astfel de lucruri nu vor ucide pe nimeni. Dar armata foloseşte şi ea o mare parte din aceste sisteme automate. De exemplu, mai mult de 90% din comunicaţiile militare se fac prin intermediul legăturilor de date comerciale. Da, banca ta şi Departamentul Apărării folosesc aceleaşi linii telefonice. Cu toate că cele mai multe astfel de date sunt trimise de la un aparat la altul fără intervenţia umană, oamenii pot interveni dacă au acces la sistem. Oricine foloseşte reţele computerizate este vulnerabil. Această exploatare a vulnerabilităţii este principala ocupaţie a războiului informaţional.

Armata, sau cel puţin cea americană, nu îşi poate permite să nu folosească reţele computerizate în ziua de azi. Prea multe arme, radare, magazii de provizii şi sedii centrale depind de viteza de funcţionare a acestor reţele. Oricine încearcă să îşi pună în funcţiune forţele armate fără aceste reţele va avea un mare dezavantaj în faţa celor care sunt conectaţi la reţea. Nu uita că primul lucru atacat în timpul Războiului din Golf din 1991 au fost reţelele de comunicare irakiene. Odată ce acestea au fost tăiate, irakienii nu şi-au mai putut reveni cu adevărat. Acela a fost un război informaţional cu bombe. Dar poţi duce, de asemenea, un război informaţional cu un PC şi o linie telefonică.

Decât să dai înapoi de frica unor PC-uri ostile sau a hackerilor rău intenţionaţi din spatele lor, mulţi dintre cei aflaţi în slujba armatei au preferat să caute metode prin care să lupte împotriva hackerilor. Urma să fie o luptă specifică. Nu a existat niciodată un război care să fie deschis unor indivizi anonimi care se află în locuri îndepărtate, înarmaţi cu un computer şi aparatură electronică. Da, au existat mulţi tocilari foarte implicaţi în alte războaie ale secolului. Al Doilea Război Mondial a avut

astfel de persoane care au creat şi de multe ori au setat radare şi aparate de măsurat electronice. Alţii au spart coduri şi au inventat instrumente letale, precum operaţiunile de cercetare. Dar cei mai mulţi dintre aceşti ţipi (erau în mare parte bărbaţi, atunci ca şi acum) erau organizaţi, chiar foarte disciplinaţi şi lucrau în condiţii de securitate extremă. Duşmanii lor sunt în mare parte necunoscuţi şi nimeni nu poate fi sigur de loialitatea lor. Un lucru este însă cert: hackerii black hat se află acolo şi fac presiuni de mai bine de două decenii. Cei mai mulţi din cei care au fost prinşi sunt suspecţii de serviciu. Aceştia sunt copiii neloiali ai clasei de mijloc. Fostele naţiuni comuniste s-au dovedit a avea şi ele câţiva cyber-cuţitari, o parte dintre ei fiind plătiţi de guvernele ţărilor lor. Dar după câte ne putem da seama, nu hackerii organizaţi au fost cei care creau viruşii şi spărgeau reţelele „sigure”. Nu, tot acest măcel era făcut de către cei care lucrau pe cont propriu. Unii dintre aceşti independenţi încheiau înţelegeri cu agenţii de spionaj pentru ideologii, bani sau doar de dragul de a face rău. Unii au fost prinşi, dar nesiguranţa dată de numărul mare al celor nedescoperiţi este motorul maniei actuale de a obţine capacitatea de a conduce războiul informaţional.

Ceea ce se pierde în toată disperarea produsă de cyber-război sunt pagubele produse sistemelor informaţionale care sunt şi au fost mereu cauzate de eroarea umană. Aceste dovezi de neloialitate vin fie din partea utilizatorilor, fie a programatorilor, a creatorilor de hardware sau a „integratorilor” (cei care ataşează hardware-ul şi software-ul). De multe ori este imposibil să îţi dai seama dacă eroarea unui sistem este rezultatul unei programări prost făcute sau al unui cip creat stângaci ori consecinţa unui atac cyber-războinic. Toate acestea au dus la crearea unor tehnici pentru diferenţierea erorilor obişnuite ale sistemelor de atacurile cyber-războinice reale (cu adevărat reale). Ceea ce face această abordare

interesantă este faptul că un atac inteligent realizat ar încerca să introducă erori în reţelele inamice care să pară erori cauzate de probleme ale hardware-ului sau software-ului. Dar abordarea cea mai cunoscută a cyber-războiului este lovirea celuilalt cu putere cu toate armele pe care le deţii. Aşadar, distruge sistemele informaţionale ale inamicului cât mai complet posibil.

Cu toate acestea, multe naţiuni văd cyber-războiul ca pe un mod de nivelare a câmpului de joacă. Un fel de altă versiune a „atacului cu armă nucleară". Dar – vai! – nu aşa funcţionează. Popoarele industrializate deţin cele mai multe computere şi cei mai mulţi hackeri. Există şi excepţii. Fostele naţiuni comuniste au educat mai mulţi oameni decât ar fi putut trimite la lucru şi aceasta a dus la crearea unui număr mare de specialişti care dispuneau de timp şi purtau ranchiună societăţii. Bulgaria, dintr-un motiv ciudat, a fost sursa multor viruşi încă din anii '80.

Popoarele noncomuniste care îi educă pe oameni fără a le asigura locuri de muncă, precum Pakistanul, au produs şi ele mulţi hackeri rău intenţionaţi.

India, pe de altă parte, şi-a pus la muncă cinstită mulţi dintre programatorii talentaţi. Deşi acest lucru a micşorat procentul programatorilor care se îndreaptă spre hacking, a furnizat Indiei o mare de abilităţi pentru cyber-război. Este posibil, şi s-a şi făcut acest lucru deja, să angajezi hackeri mercenari. Dar la fel ca în cazul oricărei arme, naţiunea cea mai bine organizată, are şi „cele mai mari batalioane", în vreme ce o mână de „superhackeri" care lucrează pentru o naţiune mai mică ar putea aduce pagube masive, să zicem, sistemului informaţional din SUA, probabilitatea ca acest lucru să se întâmple este redusă (ca şi probabilitatea de a fi lovit în cap de un meteorit în cădere). Naţiunile industrializate au luat în serios pericolele cyber-războiului, mult mai serios decât modul în care opoziţia a creat armele cyber-războinice. Cyber-războiul nu se compară cu poveştile

înspăimântătoare care aduc senzaţionalul ştirilor de peste zi. Dar nu este nimic mai mult decât acelaşi mod vechi de luptă împotriva inamicului, care a fost printre noi încă de la prima bătălie cunoscută de acum 3.200 de ani. Acolo, în sudul Libanului, hitiţii au „compromis” cu succes

„Sistemele de informaţii” egiptene cu o mulţime de informaţii înşelătoare. Acela a fost un cyber-război, sau, aşa cum mai este numit uneori, război informaţional.

CAPITOLUL 3
INTERNETUL: CREAT PENTRU A FI ATACAT

TERMENI TEHNICI

Glosarul complet, ce include şi termenii definiţi mai jos, poate fi găsit la sfârşitul cărţii.

ARPANET vine de la Advanced Research Projects Agency Network. Aşa era numit internetul în anii ’70 şi 80, când încă mai era un proiect de cercetare al Departamentului Apărării.

Apache este un program software (cunoscut şi sub numele „software server”) *Open Source Movement* (adică gratis), pentru rularea paginilor web pe un computer-gazdă. Majoritatea site-urilor web pe care le poţi vedea funcţionează cu Apache.

CRT este Cathode Ray Tube. Adică monitorul computerului. În televiziune sunt folosite tipuri diferite de CRT-uri.

Fibra optică este un tip de cablu pentru transferul datelor pe distanţe lungi. Spre deosebire de vechiul cablu (de cupru) care transfera datele prin semnale electrice, fibrele optice folosesc lumina pentru transport prin aceste bucle de cablu. Astfel pot fi transferate mult mai multe date la un preţ mai mic.

ISP înseamnă Internet Service Provider. Acestea sunt companii, precum AOL sau Earthlink, care furnizează utilizatorilor accesul la internet. De fapt, ISP-urile plătesc sume mari de bani companiilor de telefonie care construiesc şi întreţin „coloana vertebrală” a internetului pentru linii de mare capacitate, pe distanţe lungi, ce transportă cea mai mare parte a traficului pe internet (e-mail, cereri de pagini web, descărcarea fişierelor, înţelegi ce vreau să spun).

Linux este un sistem de operare gratuit creat de

programatorii *Open Source Movement.* Linux câştigă tot mai multă popularitate printre companii şi instituţii şcolare. Deşi nu este la fel de uşor de instalat şi întreţinut precum produsele comerciale (cum ar fi Microsoft Windows), software-ul este gratuit.

TCP/IP este setul de standarde al oricărui computer pentru a comunica pe internet. Orice computer cu software care a aderat la standardele TCP/IP poate fi conectat la internet. Aceasta a fost o idee radicală la vremea respectivă (anii ’70), dar era nevoie de ea pentru a deveni accesibil la scară mare.

Aparatura wireless pentru internet. La început arătau ca nişte telefoane mobile un pic mai mari, dar erau ataşate la internet în locul sistemului telefonic. Internetul a fost un accident. A început ca un proiect al guvernului pentru dezvoltarea unor idei originale pentru comunicarea datelor. Lucrurile au devenit mult mai interesante decât s-ar fi aşteptat oricine, iar după 20 de ani oamenii din afara micii comunităţi a internetului au observat ce amploare poate lua acest fenomen.

AJUNGI ORIUNDE PRIN TRANSMISIA DE PACHETE

Sistemele telefonice au în comun cu internetul transmisia datelor electronice. Cu toate că sunt controlate cu vigilenţă şi rapide, dacă vei distruge un centru de control telefonic, mii sau chiar sute de mii de oameni vor pierde accesul la acest serviciu. Acest lucru s-a întâmplat la New York, în 11 septembrie 2001. Mai multe sute de mii de utilizatori ai telefonului au pierdut accesul. Alte milioane au văzut cum serviciul telefonic are întreruperi sau nu mai funcţionează deloc. Singurele excepţii au fost în cazul utilizatorilor de aparatură de internet wireless (Blackberry în cea mai mare parte). Mesajele lor au putut fi transmise pentru că internetul a fost conceput pentru a supravieţui distrugerilor. Dacă poţi pune un mesaj pe net,

va ajunge la destinaţie (dacă acea destinaţie mai există) indiferent de cât de avariat este netul.

Internetul supravieţuieşte în orice condiţii prin transmisia de pachete, o tehnică ce divizează datele (e-mail, conversaţii telefonice, muzică sau videoclipuri) în blocuri mici sau pachete, după care le trimite (câteodată separat) către destinaţie. Pot exista întârzieri, dar în cele din urmă toate pachetele vor ajunge. Cu vechiul sistem de comutare a circuitului folosit de companiile telefonice, fie aveai o conexiune (un „circuit") cu persoana cu care vorbeai, fie nu aveai deloc. La fel ca multe idei noi, metoda rapidă de transmisie a datelor în blocuri mici a fost elaborată înainte să existe bani suficienţi sau hardware-ul necesar pentru a o pune în aplicare la o scară mai largă. Transmisia de pachete necesită mai multă capacitate (linii telefonice) decât comutarea de circuite. Dar cum companiile de comunicaţii au creat tot mai multă capacitate, era de aşteptat ca în cele din urmă transmisia pachetelor să fie pusă în practică. Şi de asta era nevoie, de multe resurse.

În principiu se împarte informaţia (care poate fi sunet, precum vocea cuiva care vorbeşte) în pachete de date (aproximativ 200 de biţi sau caractere fiecare). Fiecare pachet conţine informaţii despre destinaţie. Milioanele de computere de pe internet transmit datele printr-un computer specializat numit ruter. Aceste rutere comunică în mod constant între ele şi fiecare păstrează o listă actualizată cu cele mai eficiente căi de trimitere a mesajelor către destinaţie. Ele lucrează cu serverele locale web (PC-uri care înmagazinează sau „găzduiesc" pagini web sau alte chestii pe care le găseşti pe net) şi cu baza de date DNS (Domain Name System). Bazele de date DNS traduc numele domeniului (aol.com sau bigschool. edu) în adresă numerică. Oamenii se descurcă mai bine cu textele, dar maşinile preferă numerele.

De exemplu, dacă lucrezi la o universitate,

computerul tău este probabil conectat la reţeaua de calculatoare a universităţii. Să zicem că adresa ta de e-mail este joe@ doebigschool. edu şi că îi trimiţi un e-mail prietenului tău mybuddy@aol.com. Atunci când trimiţi acel e-mail, sistemul de calculatoare al universităţii îl trimite către ruter, care trimite pachetele ce comprimă mesajul tău către o serie de alte rutere până când ajunge la sistemul AOL, unde mesajul va fi ţinut până când prietenul tău se conectează la AOL şi îşi verifică e-mailul.

Frumuseţea acestei tehnici este că acele pachete care conţin, să zicem, un mesaj de e-mail pot călători toate printr-o serie de servere până ajung la destinaţie, unde sunt reasamblate. Aşa cum au constatat mulţi utilizatori, cele mai multe pachete ajung la destinaţie în câteva secunde. Dar uneori există probleme pe traseu (un alt lucru pe care majoritatea utilizatorilor l-au experimentat, atunci când deschid webul şi dintr-odată totul merge mai încet) şi poate dura ceva vreme până când ajung pachetele. Este de aşteptat ca lucrurile să meargă prost pe net. Câteodată, dintr-un motiv sau altul, un server nu mai funcţionează sau are loc un dezastru natural ce rupe liniile de fibră optică ce sunt responsabile pentru o mare parte din traficul internetului. De pildă, odată s-a întâmplat pentru că un constructor a tăiat din greşeală o linie de fibră optică. Astfel de lucruri încetinesc, dar nu opresc internetul. Durabilitatea internetului este în permanenţă testată. Aceste dezastre ne pot ajuta în găsirea unor soluţii pentru a diminua efectul unei astfel de probleme.

DNS-ul (Domain Name System) a apărut mai târziu în dezvoltarea internetului. A fost realizat în 1987 pentru a îngădui internetului să treacă de la statutul de operaţiune guvernamentală la o entitate publică. Unele organizaţii au fost nevoite să păstreze o evidenţă a noilor adrese web (domenii), iar ideea de a avea nume mai uşor de reţinut în locul numerelor le surâdea de ceva vreme. Compania Domain Solutions a obţinut contractul pentru a face acest

lucru, cu toate că existau câteva servere autorizate să înregistreze noile adrese de internet.

DNS ŞI ROOT SERVERELE

Deşi există baze de date DNS peste tot pe internet, autoritatea supremă o deţin cele 13 root servere DNS peste tot în lume. Sunt un element-cheie al internetului. Există un root server administrator care actualizează informaţiile pe celelalte 12 root servere o dată sau de două ori pe săptămână. Aceste root servere conţin lista principală cu numele de domenii înregistrate şi adresele lor numerice pe care toate celelalte baze de date DNS le pot consulta. Spargerea unui root server ar putea, de exemplu, să redirecţioneze traficul internetului către un site fals ce se dă drept bancă şi care, să zicem, colectează informaţii despre cărţile de credit. În ceea ce priveşte cyber-războiul, dacă toate root serverele ar fi distruse fizic, internetul ar continua să funcţioneze întrucât majoritatea numelor de domenii nu se schimbă. Nu ai putea adăuga noi adrese de internet până când root serverele nu ar fi consolidate.

E-MAILUL PREIA ARPANET

Internetul putea fi creat pe baza tehnologiei telefonice (comutarea de circuit). Aşa s-a şi întâmplat în 1969, când a trecut online prima reţea, conectând patru computere din diferite părţi ale ţării. Totuşi, în anii ’70, programatorii şi-au dat seama că software-ul folosit pentru tehnologia transmiterii de pachete, şi nu cablurile telefonice, va schimba lumea.

Cu această convingere, a fost dezvoltat e-mailul. Înainte ca primul mesaj să fie trimis în 1971 şi utilizatorii ARPANET să înceapă să îl folosească în 1972, mesajele puteau fi trimise de la un computer la altul şi nu de la o persoană la alta. Roy Tomlinson a venit cu ideea folosirii adreselor de e-mail individuale cu ajutorul noului „@” care

separa numele persoanei de sistemul computerului pe care persoana îl folosea. Oamenii puteau avea acum adrese de e-mail personale. Înainte nu puteai decât să trimiţi mesaje de la computerul Universităţii Columbia la cel al Universităţii Penn State. Cineva de la Penn State trebuia să se uite pe fiecare mesaj în parte pentru a vedea cui îi este adresat. Noul sistem îţi permitea să trimiţi e-mailuri direct de la joe@Columbia. edu la bili@pennstate. edu. Aceasta a devenit prima „aplicaţie ucigaşă”.

Funcţiona. În 1975, 75% din traficul ARPANET era ocupat de e-mailuri. Până la sfârşitul anilor ’70, utilizatorii ARPANET au fost de acord că e-mailul a schimbat totul şi că va deveni extrem de folosit în reţele. Era un lucru neanticipat şi neplanificat. Scopul iniţial al ARPANET-ului era de a permite oamenilor să folosească computerele celorlalţi şi să trimită fişiere de date de la unii la alţii. Această evoluţie neaşteptată i-a făcut pe cei implicaţi în proiect să îşi dea seama că pot apărea şi alte surprize. Aveau dreptate, iar problemele de securitate şi utilizarea internetului ca armă s-au dovedit a fi o parte din acestea.

La scurt timp a apărut un nou concept, şi anume cel al listelor de e-mail, care permitea oamenilor să îşi facă mesajele cunoscute unii altora (acum sunt cunoscute sub numele de *listserv,* care au fost dezvoltate în anii ’80). Interesant este faptul că cea mai populară astfel de listă discuta despre *science fiction.* Era un indiciu al unei alte direcţii neaşteptate spre care se îndrepta ARPANET. în 1979, primul joc *Multi-User Dungeon (MUD), MUD1,* a luat naştere în Marea Britanie (la Universitatea din Essex). Aveau să îi urmeze multe alte jocuri în reţea. Mai fuseseră şi înainte jocuri pe ARPANET, dar *MUD-urile* erau unice pentru că implicau jocul pe roluri. Jucătorii nu numai că rezolvau puzzle-uri şi se plimbau prin labirinturile *MUD-ului,* dar interacţionau şi cu alţi jucători. Studenţii de la secţia de ştiinţă a computerelor erau destinaţi să aprofundeze *MUD-urile,* pentru a crea unele noi; exista un

număr infinit de posibilităţi.

Programatorii au început să îşi îmbunătăţească încercările de programare în timpul pe care îl petreceau creându-şi *MUD-urile.* Dar au existat şi destui studenţi de la ştiinţa computerelor şi inginerie care au fost exmatriculaţi din cauza obsesiei lor. În cele din urmă, multe şcoli de inginerie au dezvoltat programe de consiliere pentru această formă de dependenţă. Nu că şcolile nu ar fi avut experienţă cu astfel de probleme; s-a descoperit că studenţii care îşi făcuseră un cont de e-mail în anii ’70 petreceau prea mult timp cu noua lor jucărie sau noul instrument, în funcţie de cum îl priveşti.

SALVAT DE UN *OPEN SOURCE* APACHE

Comunităţile e-mail au dus la creşterea extraordinar de mare a ARPANET-ului; această comunicare a creat idei de care oamenii voiau să se folosească. În cele din urmă, s-a ajuns la Usenet, care era o versiune a internetului pentru ceea ce făceau Compuserve cu forumurile şi sistemele BBS cu afişele de prezentare. De fapt, ideea BBS existase de ceva vreme, dar cum numărul oamenilor de pe net creştea, listele de e-mailuri erau suprasolicitate (prea mulţi oameni de pe liste trimiteau prea multe mesaje). Aşa că o parte din cei cu mintea limpede s-au întâlnit şi au venit cu o soluţie. Simţul comunităţii şi faptul că guvernul plătea pentru toate acestea (făcându-le „gratis”) au condus la *Open Source Movement.* Adică mii de programatori care scriau şi întreţineau (rezolvau problemele şi adăugau funcţii noi) software-ul gratis.

Ideea *Open Source* nu a fost doar o altă formă idealistă, dar neconvingătoare de mişcare din anii ’60; chiar avea un scop util şi încă mai are. Sistemul de operare Linux şi software-ul serverului Apache sunt ambele produse *open source.* Apache este cel mai des folosit (şi cel mai sigur în faţa atacurilor web). Linux este una dintre armele sistemului de operare Linux pe care funcţionează

Apache. De asemenea, Linux prezintă mai multă siguranţă decât Windows Microsoft. El nu a apărut (de fapt, GNU/Linux) până în 1993, după zece ani de muncă. Proiectul GNU a început în 1983 pentru a crea un sistem de operare gratuit. Existau deja o mulţime de instrumente *open source* disponibile. Dar fără un sistem de operare *open source,* puteai fi victima unei companii (precum Microsoft) care să îţi blocheze instrumentele *open source* cu o schimbare neaşteptată în sistemul de operare (de exemplu Windows). Totul durează mai mult atunci când foloseşti voluntari şi primele lansări ale Linux-ului şi Apache-ului nu au apărut decât abia la mijlocul anilor ’90. Deşi Linux rulează numai un sfert din serverele web (la începutul anului 2002), evoluţia lui a fost impresionantă. Cu toate acestea, Apache îl bate chiar şi pe Microsoft, rulând mai mult de jumătate din serverele web. Şi asta pe drept motiv, întrucât Apache are numai o mică parte din problemele de securitate pe care le are serverul web al Microsoft-ului, care este mai scump şi are mult mai multe erori (deşi este promovat mult mai agresiv).

Aceasta scoate în evidenţă unul din pericolele majore pentru utilizatorii de internet de azi; securitatea. Software-urile *open source,* precum Linux sau Apache, folosesc coduri mai robuste; utilizatorii îl realizează şi îl întreţin spre deosebire de o corporaţie (ca Microsoft). Problemele legate de Apache pot fi rezolvate în numai câteva ore de mulţi voluntari nerăbdători, talentaţi şi receptivi. Serverul web al Microsoft, IIS, are nevoie de cel puţin câteva zile (de obicei câteva săptămâni) pentru a rezolva problemele legate de securitate.

Dar motivul pentru care a fost creat Unix *open source* a fost datorită faptului că era un sistem de operare foarte bun. Catalogat multă vreme (într-o oarecare măsură pe bună dreptate) ca fiind sistemul de operare „făcut de tocilari pentru tocilari”, Unix a fost creat la Bell Labs la începutul anilor ’70. Se dorea ca inginerii să construiască

un sistem de operare care să poată face faţă mai multor utilizatori în acelaşi timp (un concept destul de avansat la vremea respectivă) şi care să fie uşor adaptat la computere diferite. Până la acea vreme, codul sistemului de operare era particularizat, pentru a obţine cea mai bună performanţă pentru un singur model de computer. Asta însemna că era dificil să adaptezi un sistem de operare, astfel încât să funcţioneze pe mai multe modele de calculator. Dar Unix se voia a fi sistemul de operare al viitorului, aşa că a fost creat într-un mod mai liber, făcând mult mai uşoară adaptarea lui pentru aproape orice fel de computer. La vremea aceea, era o idee radicală, dar s-a dovedit a fi o predicţie corectă a direcţiei în care se îndreptau calculatoarele. Normal, Unix a fost favorizat de mulţimea ARPANET. în anii ’80, software-ul de bază al internetului (numit TCP/IP) a fost creat în Unix. Acest lucru a făcut Unix-ul şi mai atrăgător pentru oricine dorea să pună bazele unui server de internet.

Cu software-ul TCP/IP, care era parte din Unix, nu trebuia decât să bagi în priză computerul tău şi erai pe net.

Înainte ca internetul să devină monstrul de azi, pionierii au fost nevoiţi să creeze instrumente şi funcţii de bază. Multe dintre aceste instrumente fie nu erau (şi încă nu sunt) văzute de utilizatori, fie erau luate drept sigure. E-mailul a fost iniţial creat pentru a fi un instrument, unul care în scurt timp să transformat în ceva mult mai mare. În 1973, a venit altul: FTP (File Transfer Protocol), care a reprezentat o mare îmbunătăţire. Înainte de existenţa webului, folosirea FTP-ului însemna tipărirea mai multor comenzi pentru a transfera un fişier de la un computer aflat la distanţă la al tău. FTP a fost şlefuit şi îmbunătăţit atât de mult încât, astăzi, oricine poate selecta un icon şi imediat fişierul va fi transferat. Este interesant de remarcat că o astfel de schimbare majoră a modului în care schimbăm informaţiile, bazat pe viteză, a fost

dezvoltată pentru că internetul nu era supravegheat. Cu toate acestea, astăzi, această uşurinţă de utilizare furnizează oportunităţi pentru infractori şi spărgători pentru a ajunge la PC-ul tău. Încă mai încercăm să astupăm găurile de securitate deschise acum 20 de ani, când instrumentele internetului au fost create pentru prima dată.

NU EXISTĂ SIGURANŢĂ

După cum vedem, dacă securitatea ar fi reprezentat un factor major încă de la început, internetul nu ar mai exista, sau cel puţin nu ar exista aşa cum îl ştim. Un alt exemplu cu o problemă de securitate care nu a avut însă şansa să aibă impact asupra internetului iniţial a fost exploatarea comercială a companiei Telenet asupra tehnologiei transmisiei de pachete din 1974. Reţelele comerciale (companie către companie), create de Telenet, Tymnet, Compuserve şi alte firme din anii ’70, operau foarte diferit – şi prohibitiv – de internetul în devenire, cu toate că foloseau în mare parte aceeaşi tehnologie. Securitatea lor era strictă, dar utilizatorii aveau mult mai puţină flexibilitate. Nu puteai face de unul singur instrumente pentru acele reţele, ci trebuia să îi ceri acest lucru companiei care se ocupa de aceasta. De asemenea, reţelele comerciale presupuneau mai multe costuri pentru funcţionare şi erau mai scumpe şi pentru clienţi. Diferenţele radicale au putut fi văzute în 1979, când Compuserve a pus bazele service-ului pentru clienţi. Deşi acest serviciu era scump, era mai puţin intrigant pentru utilizatori (erau mai puţine opţiuni) şi mult mai sigur decât internetul.

Anii ’60 şi 70 au adus cu ei şi minicomputerele. Componentele calculatoarelor erau mai ieftine şi a devenit posibil să creezi un computer mai puţin capabil, unul care să fie, de asemenea, mai mic (de mărimea unui frigider sau chiar o cincime din acesta). Cu toate că fiecare avea un

preţ de peste 100.000 $ la valoarea de azi, minicomputerele, la fel ca e-mailul, au fost un alt progres neanticipat care a schimbat peisajul calculatoarelor în moduri neaşteptate. Datorită lor, existau acum mult mai multe computere. Dezvoltatorii iniţiali ai internetului nu au privit reţeaua internetului ca fiind o achiziţie pentru clienţi, cel puţin nu până când (au estimat), la un moment dat în secolul XXI, activarea unui computer *mainframe* ar fi fost destul de ieftină. Dar la sfârşitul anilor ’70, minicomputerele au dat naştere PC-urilor şi modemurilor şi au dus la scăderea preţului tehnologiei, care putea fi cumpărată şi de cei din clasa de mijloc.

Sosirea PC-urilor a condus de asemenea la împărţirea regatului tocilarilor în două secţiuni, mulţimea „marele fier” (*mainframe*) şi oamenii PC-urilor. Această bătălie epică a luat sfârşit de curând cu ambele părţi ieşind câştigătoare (sau ambele pierzând, depinde cum priveşti lucrurile, dar acesta este subiectul unei alte cărţi).

Dezvoltatorii ARPANET au crescut cu şi au lucrat la sisteme pentru computere mari care aveau terminale „proaste”. Un pic mai mult decât un CÂT alb-negru, o tastatură şi suficiente electronice pentru a-l face să vorbească cu un *mainframe* (care stoca toate datele şi efectua toate funcţiile), aceste ataşamente aveau preţuri mici. Aminteşte-ţi că în anii ’70 electronicele erau scumpe; acele terminale proaste costau numai 5.000 – 15.000 $ în banii de azi comparativ cu preţul unui *mainframe* de jumătate de milion de dolari (şi chiar mai mult, până la zeci de milioane de dolari). Cu toate acestea, la vremea respectivă, acesta era modul cel mai practic de a facilita oamenilor accesul la calculator. Sistemul de operare Unix, care a susţinut internetul încă de la început, a fost realizat pentru a face faţă mai multor utilizatori la acelaşi computer. Ulterior, internetul a adăugat capacitatea de a face acest lucru şi pentru utilizatorii care comunicau printr-un modem pe o reţea telefonică, dar şi pentru cei

care foloseau un terminal ataşat printr-un cablu de *mainframe* din apropiere. Primele PC-uri care au apărut la sfârşitul anilor ’70 erau chiar mai ieftine decât terminalele proaste (2.500 – 5.000 $ în banii de azi), dar încă erau privite ca fiind nişte jucării scumpe de majoritatea profesioniştilor în calculatoare. În 1980, era ceva obişnuit pentru utilizatorii de PC-uri să folosească în mod egal modemuri ieftine pentru a se conecta la sistemele BBS rulate de PC-uri. Se stabilise un punct de sprijin. Nu a durat mult până când utilizatorii ARPANET şi-au dat seama că pot folosi această combinaţie pentru a se conecta de acasă. În 1982, doi utilizatori de PC, nişte adolescenţi din Los Angeles, şi-au dat seama de acelaşi lucru. Exista o singură problemă: nu erau utilizatori ARPANET autorizaţi. Puştii au luat-o razna şi asta a întărit atitudinea multor dezvoltatori ARPANET că PC-urile erau unealta diavolului.

Profesioniştii „de procesare de date” (DP) care conduceau sistemele *mainframe* au încercat să ţină PC-urile departe de organizaţiile lor în timpul anilor ’80. Nu considerau PC-urile „computere reale” şi vedeau răspândirea lor ca o ameninţare a modului în care se făceau calculatoarele până atunci. Dar au pierdut acea bătălie, apoi, reţelele locale (LAN-urile) au funcţionat numai cu PC-uri. Din nou, comunitatea procesatorilor de date s-a uitat superior la această dezvoltare demnă de milă şi îşi doreau ca ea să dispară. Dar nu a făcut-o. Profesioniştii DP au crezut că este periculos ca o mână de amatori să pună mâna pe computerele lor. Utilizatorii, care în acest caz erau departamentele din marile corporaţii, au văzut diferenţa de preţ dintre PC-uri şi *main-frame-uri,* lucru care a condus, în cele din urmă, la pierderea bătăliei de către *mainframe*-uri. În plus, s-a schimbat şi percepţia asupra lor.

Din motive practice, *mainframe-ul* devenea un dinozaur, cu toate că susţinătorii săi spuneau că PC-urile sunt mult mai puţin de încredere, ceea ce era adevărat.

Dar nu asta conta. PC-urile convingeau prin preţurile scăzute, iar utilizatorii erau mai dispuşi să accepte un grad mai mic de siguranţă. *Mainframe-urile* încă aveau un mecanism de comunicaţii scump, care permitea conexiunea cu terminale proaste, chiar pentru utilizatorii la distanţă prin intermediul ARPANET şi alte reţele. Sigur că aveau şi o capacitate mai mare (şi foarte scumpă). De exemplu, un model de hard drive de 75 megabiţi de la sfârşitul anilor ’70 costa în jur de 40.000 $ la valoarea de astăzi. PC-urile de la început nu aveau nevoie de toate acele componente scumpe.

Cu toate acestea, nu era un război de tipul „eşti cu noi sau împotriva noastră”. Foarte mult timp, cei care susţineau *mainframe-urile* au avut un PC acasă sau chiar au sugerat introducerea lor în departamentele DP.

În acelaşi timp, mulţi maniaci ai PC-urilor nu aveau niciun fel de problemă să folosească *mainframe-urile* (la urma urmei, Compuserve şi internetul rulau pe *mainframe-uri).* Ceea ce a dus la încheierea disputei au fost avantajele pe care le aducea conectarea acelor LAN-uri la *mainframe-uri.* Totuşi, conceptul de *mainframe* s-a schimbat ulterior. Creatorii au observat că producătorii de PC-uri adăugau componente *mainframe* analoage (precum hard diskuri mai mari) la preţuri mai mici. În anii ’90, lucrurile s-au inversat: *mainframe-urile* erau construite cu componente de PC. Putem spune că PC-urile au crescut în capacitate pentru a întâmpina nevoile inginerilor şi ale oamenilor de ştiinţă, iar în prezent, cele mai puternice PC-uri sunt descrise ca fiind *mainframe-uri.*

Dar a existat şi un dezavantaj. Una dintre diversele probleme pentru care susţinătorii PC-urilor şi ai *mainframe-urilor* s-au bătut cap în cap a fost „controlul”. Adepţii mai vechi ai *mainframe-urilor* veneau dintr-o perioadă (anii ’50) în care computerele erau noi, scumpe şi instabile. Trebuiau protejate şi folosite cu grijă. Timpul însemna bani, iar accesul nu le era permis celor neiniţiaţi

sau neexperimentaţi. Partizanii PC-urilor, pe de altă parte, au promovat libertatea personală, au luptat pentru a dărâma zidul fobiei tehnologice şi au căutat să îşi folosească computerele aşa cum voiau. Lupta a început să se dea pentru practicile de securitate *versus* lipsa lor. Desigur că existau multe elemente de siguranţă integrate în PC-uri, dar ele puteau fi uşor înfrânte de orice maniac care îşi merita numele. Pentru *mainframe-uri,* securitatea era religie. Pentru utilizatorii de PC-uri, era o glumă. Apoi a apărut internetul. Oamenii au început să facă cumpărături online, făceau operaţiuni bancare în spaţiul cibernetic şi vindeau acţiuni pe site-uri web. Securitatea reţelelor nu mai era ceva de care să se ocupe bătrânele *mainframe-uri,* mai ales dacă licitai obiecte de colecţie pe e-Bay sau îţi făceai toate operaţiunile bancare pe site-uri. Nu mai era timp de întoarcere, iar repararea pagubelor avea să ia mult timp.

Slaba securitate a internetului nu este numai rezultatul războiului dintre PC-uri şi *mainframe-uri.* Cultura ARPANET a jucat şi ea un rol. Deşi comunitatea *open source* a făcut foarte multe pentru asigurarea securităţii pe net, natura libertină, cooperantă şi atmosfera de încredere a internetului de la început au contribuit şi ele la problemele actuale. Pentru a asigura funcţionarea internetului, o mare parte din această deschidere şi cooperarea erau necesare. Dar pe atunci puteai avea încredere în aproape oricine că va lăsa webul aşa cum era, dacă nu chiar mai bun. Nu acelaşi lucru se întâmplă şi astăzi.

ARPANET SE DEZLĂNŢUIE

Deşi ARPANET era crud şi încă doar o reţea experimentală, în anii ’70, a funcţionat. Îţi crea dependenţă. Oamenii îl doreau. Cererea tot mai mare pentru acces la internet a dus la înfiinţarea NSFNet (National Science Foundation Net) în 1985 pentru aceia

din domeniu care nu erau parte a proiectului ARPANET ce se afla în dezvoltare. Agitaţia din campus dusese deja la crearea Computer Science Network (CSNET) şi a BITNET (Because It's Time Network) în 81 – 82. În 1985, Departamentul Apărării, care se despărţise de ARPANET în 1983 pentru a crea MILNET (numai pentru armată), a renunţat definitiv la controlul asupra ARPANET.

O altă dezvoltare crucială la începutul anilor '80 a fost crearea TCP/IP ca standard ARPANET pentru software-ul de comunicare. TCP/IP a evoluat încă de la începutul anilor '70 ca un set de reguli robuste şi flexibile pentru software („protocoale", cum ar spune tocilarii) care au înlesnit conectarea la ARPANET-ul guvernului a oricărei reţele de calculatoare (şi existau zeci de tipuri şi variante). BITNET nu a folosit TCP/IP, dar CSNET a făcut-o şi, în consecinţă, era conectat la ARPANET cu succes (şi câteva dureri de cap) în 1983. În 1984, NSF (Naţional Science Foundation) a preluat conducerea de la ARPANET sau ceea ce se numea deja internet. În acelaşi an, DNS a fost dat în folosinţă, facilitând utilizatorilor identificarea şi accesarea unui site web. În 1985, ARPANET a devenit oficial NSFNet (National Science Foundation Net). Netul era acum o operaţiune civilă. Dar nu numai numele a fost schimbat. Dintr-odată erau mult mai mulţi oameni pe internet. În 1981, existau 213 computere-gazdă (gândeşte-te la ele ca la servere) conectate la ARPANET. În 1983, acest număr a urcat la 562 şi s-a dublat în 1984 la 1.024. În 1985, anul în care internetul a fost deschis pentru public, existau 1.961 de computere-gazdă. Dar în 1987 erau 28.174, iar în 1988 peste 56.000. Până în 1990 erau deja 300.000. În acel moment, ARPANET a fost desfiinţat şi nu a mai rămas decât internetul. Nu mai erai nevoit să şterpeleşti un cont de la o universitate sau de la un centru de cercetare pentru a intra pe internet. Acum puteai cumpăra acces lunar printr-un ISP (Internet Service Provider). Aceasta a condus la o creştere spectaculoasă până în 1995, când a

fost lansat World Wide Web; existau 6, 6 milioane de computere-gazdă.

Această creştere bruscă şi rapidă a internetului a dus la dezvoltarea unor noi instrumente care să facă faţă tuturor elementelor noi care apăreau pe net. Primele motoare de căutare erau numite Gopher, Archie, Veronica şi WAIS şi permiteau oamenilor să caute pe net şi să recupereze documente şi fişiere. Plimbarea pe internet a fost numită iniţial „navigare" în 1992. Majoritatea utilizatorilor nu aveau o interfaţă grafică precum Windows sau MacIntosh. Asta era înainte ca World Wide Web să fie lansat. Era o variantă mai simplă, dar mai greu de folosit decât webul (cum au numit oamenii World Wide Webul atunci când a apărut, dar şi internetul în general). Dar NSF nu prevăzuse acest lucru. La acea vreme, NFS credea că webul trebuie să îşi extindă infrastructura, iar netul să fie folosit de cât mai mulţi utilizatori cu putinţă. NSF a negociat o mulţime de înţelegeri cu implicaţii pe termen lung, precum:

— TCP/IP a devenit obligatoriu pentru oricine voia să se conecteze la internet (toată lumea îi spunea aşa). Acest lucru a dus la evitarea unei lupte între alte câteva protocoale comerciale. Dezavantajul este că TCP/IP nu prezintă la fel de multă siguranţă în faţa hackerilor ca mulţi dintre competitorii comerciali. Dar cu TCP/IP mai mulţi oameni aveau să aibă un acces mai rapid la internet.

— Guvernul şi corporaţiile aveau să colaboreze pentru a forma „coloana vertebrală a internetului" (linii telefonice de înaltă capa citate care să transporte cea mai mare parte a traficului pe internet pe distanţe mari). De fapt acesta era sistemul de telefonie privată. Sistemul obişnuit de telefonie era folosit numai pentru „ultima milă" de la o conexiune centrală către utilizatori individuali sau reţele locale.

— Nu aveau să se calculeze preţuri între diferite neţuri. Era o propunere riscantă întrucât internetul era

încă o operaţiune comercială. Dar a simplificat lucrurile şi a ajutat la dezvoltarea rapidă a internetului. Coloana vertebrală avea să plătească singură prin taxarea oamenilor de mijloc (Internet Service Provider-ii sau utilizatorii importanţi – corporaţii, universităţi, agenţii guvernamentale) pentru accesul direct.

— Înfiinţarea Internet Activities Board (IAB) pentru a supraveghea şi încuraja cooperarea în cercetare (în SUA şi peste ocean) pentru dezvoltarea noilor tehnologii de care avea nevoie netul pentru a se extinde. Era un fel de mişcare *open source* oficială, iar IAB era un descendent direct al unei organizaţii similare (Internetworking Working Group) înfiinţate în 1992 pentru a face acelaşi lucru.

Era un început. Apoi a apărut primul val de infracţiuni pe internet. O examinare a 300 de corporaţii importante şi agenţii guvernamentale din 1987 a arătat că cinci la sută dintre ele fuseseră victime ale infracţiunilor pe calculator în anul anterior. Pierderile erau între 145 şi 730 de milioane de dolari. Cea mai mare parte erau delapidări de fonduri, transferul electronic al banilor către contul unei bănci false (contul era imediat şters pentru ca hoţul să poată scăpa). Un alt studiu vizând 300 de site-uri din 1991 a indicat că 72% din acestea suferiseră un „incident de securitate” în ultimul an. Până la acea vreme, operatorii de site-uri deveneau tot mai alarmaţi de pericol şi numai 43 au declarat că acele incidente ajunseseră suficient de departe pentru a fi considerate infracţiuni. Alte studii au arătat că numai aproximativ cinci la sută din aceste infracţiuni pe calculator au fost raportate poliţiei.

Începutul anilor ’90 a fost o perioadă haotică pentru internet. Ajunseseră să fie milioane de noi utilizatori care accesau mediul online. A fost introdus un nou software pentru a face faţă activităţii în creştere şi problemelor de securitate. Problema cel mai des întâlnită era legată de parole. În vreme ce hackingul din exterior primea cea mai

mare atenţie din partea mass-mediei, studiile au indicat că aproape 90% din infracţiuni sunt comise de cei din interior. Cele mai multe companii au considerat pierderile provocate de securitate ca pe un alt cost al activităţii şi au luat măsuri pentru îmbunătăţirea acesteia. Cu toate acestea, agenţiile guvernamentale erau preocupate de un alt aspect, ele se temeau de expunerea în faţa mass-mediei, dăunătoare din punct de vedere politic. Aceasta era o situaţie „veşti bune, veşti rele”. Vestea bună era că nu existau dezastre majore. Asta în ciuda faptului că site-urile care controlau barajele şi alte utilităţi erau sparte. Vestea rea era că aceste site-uri erau compromise şi era evident că nu este nevoie de prea mult talent pentru a face acest lucru

VALUL DE ENTUZIASM LANSAT DE WORLD WIDE WEB

La începutul anilor ’60, când a fost auzit pentru prima dată cuvântul „internet”, a început să fie concepută o altă tehnologie uimitoare. Era vorba despre hipertext şi a stagnat la stadiul de curiozitate academică până când cercetătorii de la CERN (un institut de cercetări ştiinţifice din Elveţia) au început să caute un mod mai simplu de a face schimb de informaţii pe internet. Acest lucru includea de multe ori ilustraţii şi fotografii sau articole tehnice cu o mulţime de note de subsol. Ca răspuns, Tim Berners-Lee a inventat practic World Wide Webul prin dezvoltarea ideii de HTML (Hyper Text Markup Language) şi de URL (Universal Resource Locators. Acestea sunt adrese de internet care încep cu HTTP, care înseamnă Hypertext Transfer Protocol). Normal, era nevoie de un program de comunicare special, care la scurt timp a fost numit motor de căutare, pentru a activa instrucţiunile HTML de comunicare pe internet. A durat trei ani până să fie lansate primul HTML şi software-ul care să facă acest lucru posibil. Primul server web (un computer-gazdă conectat la

internet şi programat să răspundă cererilor venite de la motorul de căutare) a fost trecut online în 1991. La început, webul era format numai din texte. Graficele, care aveau nevoie de o mai mare perioadă de timp pentru a fi încărcate, au apărut mai târziu, întrucât erau disponibile mai multe modemuri cu o viteză mai mare. Webul a avut un succes imediat, până în 1992 existau deja 50 de servere web. În 2001 erau mai mult de 24 de milioane şi mai mult de un miliard de pagini web disponibile.

În 1993, a fost creat primul motor de căutare grafic (Mozaic) de către studenţii de la Universitatea din Illinois (inclusiv Marc Andreesen, fondatorul Netscape). Motoarele de căutare Mozaic au fost lansate pentru sistemele Windows, MacIntosh şi Unix. În 1994 a fost fondat Netscape, dar goana după aur începuse deja. PC-uri mai ieftine, o versiune a Windows Microsoft (care prezenta încredere), toate îmbinate pentru a crea o altă tehnologie populară care să schimbe totul. Asemenea telegrafului, radioului şi televiziunii de dinainte, combinaţia PC/web a adus computerele la dispoziţia maselor într-un mod cu totul neaşteptat. Guvernul SUA a urcat în carusel contribuind cu 1, 5 miliarde de dolari la NSF pentru a stimula creşterea internetului, ce trebuie să fie suficient de rapidă pentru a face faţă cererilor. Internetul a crescut de la aproximativ o mie de reţele în 1985 până la peste 60.000 în 1994.

Nimeni nu avea o statistică a celor care foloseau internetul în 1995, dar era evident că se ajungea la un număr de zeci de milioane (poate chiar 40 de milioane) şi continua să crească. Principalele reţele comerciale, precum Compuserve şi AOL, s-au conectat la internet în acelaşi an, iar NSF s-a retras din afacerea netului, care a devenit o operaţiune în întregime comercială.

Încă din 1995, un studiu despre site-urile web existente a subliniat că această nouă „utilitate informaţională” făcea ceea ce sperase toată lumea: o

împărţire al 100 de site-uri alese aleatoriu. Aceasta arăta cam aşa:

Funcţia site-ului web	Site-uri care folosesc acea
Relaţii publice	21, 93%
Publicitate	20, 70%
Date bancare/Informaţii generale	9, 74%
Ştiri	9, 74%
Servicii/Informaţii despre	9, 30%
Buletin/Departament	8, 86%
Arhive/Expoziţii	6, 93%
Divertisment	6, 84%
Comentarii	4, 65%
Diverse/Altele	1, 32%

Toate acestea se petreceau înainte să apară pe web paginile personale, comerţul online şi paginile porno. Dar a mai apărut şi altceva: utilizarea tot mai frecventă a scriptării. Era un instrument antic pentru utilizatorii de computere experimentaţi şi pentru administratori. Fişierele DOS batch (fişiere, bat) erau cel mai utilizat limbaj de scripting, dar altele sunt atât de puternice încât pentru a le manevra ai nevoie de o adevărată îndemânare pentru programare. În 1995, a apărut Javascript. HTML era foarte flexibil, dar necesita scripting, iar Javascript le-a permis creatorilor de pagini web experimentaţi să îşi facă site-urile şi mai folositoare cu ajutorul scriptării. Totuşi, Javascript (şi alte instrumente asemănătoare) le-a oferit hackerilor rău intenţionaţi şi altor vandali de web un instrument puternic cu care să poată produce pagube.

Webul a furnizat o şi mai mare capacitate letală prin numărul imens de software-uri noi care erau create pentru net. Toate aceste programe tindeau să aibă erori (orice variantă nouă de software are defecte) care permiteau hackerilor să aibă acces ilegal la site. Programatorii nu au găsit prea multe astfel de defecte pentru că problemele nu afectau ceea ce programul trebuia să facă. Dar tipii răi ştiau să profite de o ocazie atunci când se ivea şi au început să creeze instrumente care să depisteze problemele de securitate. Mai simplu spus, world wide web este o variantă mult mai puţin sigură a internetului.

Dar nu se putea face cale întoarsă. Internetul nu aparţinea niciunei organizaţii. De fapt, nimeni nu era răspunzător. Aşa că nu exista o autoritate care să impună standarde de securitate. Internetul a fost creat pentru a inspira anarhia, iar rata creşterii înregistrată la sfârşitul anilor ’90 ar fi făcut dificilă implementarea oricărei politici de securitate.

Webul aduce de asemenea comerţul pe internet. Deşi acesta nu fusese încă lansat, în 1996 ISP urile au depăşit trei miliarde de dolari, iar o treime din această sumă era înregistrată în afara SUA.

În 1997 existau peste 50.000 de pagini web de comerţ, iar numărul lor în cadrul corporaţiilor private şi al reţelelor guvernamentale era în creştere. Până la sfârşitul secolului, numărul computerelor-gazdă crescuse la 93 de milioane (de la patru în 1969). Existau patru milioane de domenii înregistrate şi se estima că aproximativ 23 de milioane de oameni erau online în orice zi a săptămânii.

Dar netul nu era sigur. Poate că nu a fost creat pentru a prezenta siguranţă şi poate era destul de robust pentru a rezista oricărui asalt. Dar pericolele erau reale, iar utilizatorii lor deveneau din ce în ce mai îngrijoraţi cu privire la cel mai mare rău care se putea întâmpla.

CAPITOLUL 4 ISTORICUL CYBER-

RĂZBOAIELOR

TERMENI TEHNICI

Glosarul complet, ce include şi termenii definiţi mai jos, poate fi găsit la sfârşitul cărţii.

Adresa IP – „Internet Protocol Address”, adică ceea ce fiecare computer conectat la internet trebuie să aibă pentru a putea comunica instant cu altul. Gândeşte-te la ea ca şi cum ar fi

„Numărul de telefon” al internetului.

Bombe inteligente – vechile bombe obişnuite (învelişuri de metal umplute cu explozibili şi aruncate din avion), cu dispozitive de ghidare ataşate. Acestea conţin mici aripioare alimentate de baterii şi comandate cu ajutorul unui sistem de ghidare. Bombele obişnuite nu sunt foarte exacte, putând ateriza chiar şi la o distanţă de o sută de metri de ţintă. Bombele inteligente au o eroare de până la zece metri.

Virusul este un program pentru calculator care, odată infiltrat în computerul tău, va încerca să se răspândească şi în altele prin lista ta de adrese de e-mail şi va face alte lucruri neplăcute computerului tău. În funcţie de fiecare virus (până în 2001 au fost identificaţi 70.000), acesta poate să nu prezinte niciun pericol sau să îţi distrugă toate datele de pe hard drive.

Internetul a furnizat o nouă modalitate de a comunica, dar n-a trecut mult timp şi a devenit un câmp de luptă. Un adevărat câmp de luptă. De la Războiul Civil american încoace, a fost evident că informaţiile transmise electronic au avut rolul lor în câştigarea războaielor. În trecut, informaţiile erau importante, dar acum, cu ajutorul telegrafului, mesajele circulă cu viteza luminii. Actualmente, armata a realizat că dispune de ceva mai mult decât un simplu instrument de comunicare şi propagandă. Există două tipuri de luptă pe web. Există „războiul informaţional” tradiţional, care face tot felul de lucruri cu ştirile, fapt ce nu era posibil înainte de apariţia

webului. Şi mai există cyber-războiul, care de asemenea foloseşte webul, aşa cum îi place infanteriei să spună, „pentru a distruge lucruri şi a omorî oameni”. Din punct de vedere tehnic, cyber-războiul înseamnă folosirea în luptă a aparaturii electronice. Acest lucru, se pare, nu este o idee recentă. Din această perspectivă, cyber-războiul are deja o istorie de 60 de ani.

CEL MAI MARE CYBER-RĂZBOI

Cel mai rău lucru care se poate întâmpla în viitor este ca vreunul dintre marii cyber-războinici să dea lovitura. Un cyber-război major ar fi fără precedent. De fapt, nu, nu ar fi. Un război major care să utilizeze internetul ar fi unic, dar o operaţiune militară importantă care să folosească arme electronice a avut loc acum multă vreme, în timpul celui de-al Doilea Război Mondial. Din 1940 până în 1945, spaţiul aerian de deasupra Europei a fost împânzit de sute de mii de aeronave. Majoritatea foloseau radioul, multe aveau propriul radar, iar altele deţineau o colecţie în creştere de staţii de bruiaj, echipament de navigare electronică şi ceea ce numim azi generator de război electronic. Acesta a fost primul cyber-război. A fost imens. A durat vreme de şase ani. Şi putem afla multe despre un viitor cyber-război dacă privim înapoi la această experienţă din al Doilea Război Mondial.

La începutul celui de-al Doilea Război Mondial (1939), aeronavele aveau la bord puţin echipament electronic, format în general dintr-un radio, dar multe naţiuni nu îşi echipau avioanele nici măcar cu acesta. Dar în anii ’30 se dezvolta multă aparatură electronică nouă în laboratoare şi universităţi. Nevoile războiului au determinat utilizarea rapidă a unor aparate experimentale. Acest lucru a condus la o adevărată întrecere a armelor electronice, neegalată în viteză (în privinţa inovaţiei) sau violenţă (modul de utilizare a lor).

Acum, după şaizeci de ani, ne confruntăm cu o situaţie asemănătoare. Avem o nouă tehnologie (internetul)

care încă nu a fost încercată în război. Avem posibilitatea de a modifica rapid internetul pentru a veni în întâmpinarea nevoilor impuse de război. Internetul a fost conceput pentru a putea fi rapid modificat. Aşadar ce se va întâmpla? Hai să aflăm uitându-ne mai atent la primul mare război electronic.

Începutul războiului electronic deasupra Europei în anii ’40 a fost declanşat de efortul germanilor şi al aliaţilor de a-şi bombarda reciproc oraşele şi fabricile. Repet, era ceva unic în istorie. Existaseră unele raiduri mai mici, mai mult enervante decât distrugătoare, la sfârşitul Primului Război Mondial dar acum bombardierele erau mai mari, mai numeroase şi mai variate. Lipsurile erau suplinite printr-o gamă largă de aparatură electronică.

Printre primele astfel de aparate electronice moderne care au fost introduse în lupta asupra Europei a fost şi Knickebeinul nemţesc, în februarie 1940. Era un sistem central de navigaţie care folosea semnale de la transmiţătoarele de la sol. Acest lucru permitea bombelor aruncate pe timp de noapte să găsească ţinta şi să o atace cu precizie. Era o metodă clasică, folosită adeseori în cazul unei situaţii militare neaşteptate (bombardarea pe timpul nopţii), care aducea o soluţie tehnică pentru o problemă aparent nerezolvabilă (găsirea ţintelor pe timpul nopţii).

Deşi germanii au iniţiat bombardarea oraşelor în anii ’30, mai ales în timpul Războiului Civil din Spania (1936 – 1939), ei au crezut mereu că vor fi primii care vor înlătura luptătorii inamici, după care vor trimite bombe cu ţinte precise în timpul zilei. Atunci când Luftwaffe (forţele aeriene germane) a dat peste RAF (forţele aeriene regale din Marea Britanie) în 1940, a devenit repede evident că luptătorii englezi puteau face din bombardarea pe timp de zi o afacere scump plătită. Bombardarea pe timp de noapte evita luptătorii, dar crea probleme de navigaţie insurmontabile. Astfel a început dezvoltarea rapidă şi introducerea Knickebeinului. Pe cât de repede a fost creat,

pe atât de puţin a durat până a fost distrus. Englezii au trecut în septembrie 1940 la contraatac: Asperin. Nu erau decât nişte emiţătoare de bruiaj electronice care trimiteau zgomote pe aceleaşi frecvenţe ca şi Knickebeinul, făcându-l pe acesta din urmă inutil.

Knickebeinul era ceva de care inginerii de aeronave erau interesaţi încă dinaintea războiului din motive pur comerciale. Un astfel de sistem putea muta cu uşurinţă aeronavele comerciale dintr-un oraş în altul. Chiar şi înainte de război, utilizarea acestuia permitea avioanelor să aterizeze atunci când din cauza vremii pista nu era vizibilă. Pe baza experienţei din al Doilea Război Mondial cu aparatura de navigaţie electronică, după război a fost construit LORAN (LOng RAnge Navigation system) care este încă folosit. Deficienţele LORAN au condus la crearea GPS-ului, care foloseşte convergenţa semnalelor de la trei sateliţi spaţiali pentru a indica locul în care te afli. Acest lucru arată cât de repede pot trece tehnologiile militare şi civile de la război la pace. Nimeni nu a aflat câte întrebuinţări militare poate avea internetul şi acest fapt sperie armata.

În timpul anilor 1942 şi 1943, germanii şi englezii şi-au îmbunătăţit rapid radarele şi sistemele de comunicare. Radarele au fost create într-o gamă largă pentru a localiza cât mai exact navele aeriene.

Dar cu sute de aeronave pe cer în timpul zilei, a devenit evident că operatorii de radar aveau nevoie de o modalitate de a-i diferenţia pe tipii răi de cei buni. Astfel s-a inventat IFF-ul (Identification, Friend of Foe). Era un transmiţător radio (numit „emiţător de identificare”) care trimitea în mod constant un mesaj codat ce stabilea dacă aeronava era prietenoasă (mesajul era schimbat în mod frecvent pentru ca inamicul să nu îl poată copia şi folosi pentru a trece de defensivă).

Până la sfârşitul anilor ’90, internetul a redescoperit nevoia de IFF. Internetul foloseşte o formă de IFF în modul

în care îi autentifică pe toţi cei care sunt pe net. Nu doar parolele, ci şi datele de control trimise între server şi software-ul care rulează netul, toate folosesc o formă de IFF pentru a preveni situaţia în care cineva ar opri sau prelua anumite părţi ale internetului. La început, comunicarea pe internet se baza pe un anumit grad de încredere. Dar acum utilizatorii nu mai sunt doar un grup restrâns de cercetători, ci sute de milioane de oameni, şi nu doar câteva guverne văd internetul ca pe un posibil câmp de luptă. „Înşelătoria" (editarea unui element sau chiar a unui e-mail pentru a-l face să pară că vine din altă parte) a devenit o problemă majoră. IFF-ul englez din cel de-al Doilea Război Mondial era o soluţie simplă în comparaţie cu ceea ce trebuie făcut pe internet pentru a obţine acelaşi grad de asigurare că ceea ce vezi este adevărat. Dar efortul de a dezvolta un IFF mai bun continuă şi internetul nu va fi cu mult mai sigur până nu va fi creată o astfel de versiune.

Germanii din cel de-al Doilea Război Mondial şi-au dat seama până la urmă de IFF şi l-au folosit în scop personal, dar în alte cazuri germanii nu au realizat că aliaţii foloseau tehnologie superioară. Un bun exemplu a fost radarul cu microunde. A reprezentat o îmbunătăţire esenţială a tehnologiei de radar, care a făcut echipamentul mai puternic, dar şi de mai mici dimensiuni. Este interesant faptul că tehnologia electronică de maximă importanţă nu a fost descoperită de naţiunile care aveau cu adevărat nevoie de ea. Germanii au pus mâna pe secretul radarului cu microunde de la englezi imediat ce au avut ocazia, dar japonezii aflaseră dinainte acest lucru şi nu s-au deranjat să împărtăşească aliaţilor descoperirea lor. Internetul şi cyber-războiul vor abunda de astfel de surprize tehnice neplăcute. Problema este că va trebui să aşteptăm pentru un anumit tip de război (unul obişnuit, cu împuşcături, sau un conflict pur cibernetic) pentru a afla ce arme deţine fiecare. Nu va dura mult până când acestea

vor fi preluate de Hollywood şi vom vedea filme de spionaj unde marele secret este un fel de cyber-armă devastatoare pe internet. În acest caz, nu va mai fi vorba despre o ficţiune hollywoodiană, ci de o adevărată panică în rândul comunităţii cyber-războinice.

Lupta cibernetică din timpul celui de-al Doilea Război Mondial a arătat de asemenea şi că tehnologia mai slab dezvoltată poate fi încă folosită împotriva înaltei tehnologii. De exemplu, germanii au descoperit modalitatea de a folosi luminile pentru cercetare (setate pe o distanţă lungă), o formă primitivă de radar care nu putea fi bruiată. Aliaţii au descoperit şi ei că, dacă arunci sute de kilograme de fâşii de folie de aluminiu (numite de atunci „confetti”), creezi un nor imens în faţa monitoarelor de radar inamice. De fapt, orbeai radarul inamic. Toate acestea erau tehnologii primitive, dar făceau radarele de înaltă clasă să devină inutile, cel puţin până când bucăţile de folie ajungeau la sol. Alte idei de acest gen au avut mai puţin succes. De exemplu, englezii ştiau că nemţii se bazau pe o reţea de observatori tereştri care stăteau de veghe pe timp de noapte şi ascultau sunetul motoarelor de bombardiere. Aceştia transmiteau informaţiile sediului central, unde erau puse cap la cap toate rapoartele şi se stabilea de unde vin acele bombardiere şi încotro se îndreaptă. Englezii au încercat să perturbe acest sistem modificând sunetul pe care îl scoteau bombardierele lor, astfel încât să fie mai puternic decât de obicei. Se credea că astfel îi vor face pe observatori să predea rapoarte eronate. Nu a funcţionat. Dar trebuia încercat.

Fâşiile de aluminiu au reprezentat o tactică ce a funcţionat în 1942 şi va fi la fel de bine folosită şi în secolul XXI. încă mai există metode rudimentare pentru a face faţă inamicilor care au avantajul tehnologiei de ultimă generaţie. De exemplu, pentru a întreţine o reţea care poate comunica prin internet, dar care să fie imună la atacurile de pe net, multe organizaţii au recurs la o

conexiune

„Pe furiş”. Adică netul intern foloseşte tehnologia internetului, dar toate e-mailurile care vin sau pleacă sunt copiate pe un CD şi duse la un PC conectat la internet. Acolo, un program special preia mesajele şi le trimite pe net. Mesajele primite sunt retrimise la un PC unde sunt verificare de viruşi, după care ajung la destinatar. Nu sunt permise ataşamentele (deşi există unele excepţii în situaţia în care sunt scanate înainte de a fi trimise). Este o măsură dură, dar eficientă. Perfectă pentru administratorii de sistem a căror paranoia nu este lipsită de temei.

Din 1943 până la sfârşitul războiului, aliaţii şi germanii au dezvoltat noi radare, noi aparate de detectare sau de bruiere a lor, mai multe echipamente de navigaţie electronică (inclusiv radarul care putea crea o hartă cu ce se afla la sol) şi aparate care detectau utilizarea acestora sau pur şi simplu le bruiau. Până la sfârşitul războiului, cei implicaţi în războiul electronic aşteptau un nou element care să reziste măcar câteva luni înainte ca inamicul să contracareze. Astfel s-au impus tonul şi ritmul pentru războiul electronic care continuă şi azi.

Bruierea şi înşelătoria (inducerea în eroare în legătură cu ceva, cum ar fi zgomotul crescut al motoarelor) au devenit arme standard pentru cyber-războinici. DDOS (Distributed Denial of Service Attack) este o formă cunoscută de bruiere care blochează site-ul web ţintit. Înşelătoria este un element-cheie în hacking, întrucât implică o colecţie de tehnici care ascund activităţile hackerului, făcând identificarea acestuia dificilă.

În concluzie, măsurile noi urmate de contramăsuri reprezintă modul tipic în care este dus cyber-războiul în prezent. Uneori se duce la vedere, ca atunci când Microsoft a încercat să obţină propriul sistem de mesagerie instant conectat la mult mai dezvoltatul sistem de mesagerie al AOL. Deşi avocaţii au dezbătut această problemă în justiţie, programatorii MSN au continuat să

găsească deficienţe în software-ul AOL care permitea utilizatorilor MSN să trimită mesaje instant către utilizatorii AOL. Apoi programatorii AOL au remediat deficienţa şi au blocat accesul utilizatorilor de mesagerie instant MSN. Programatorii MSN au găsit însă ulterior o altă modalitate de intrare. În cele din urmă, avocaţii au câştigat, dar a fost distractiv de urmărit întregul proces.

Experienţa din cel de-al Doilea Război Mondial furnizează de asemenea exemple despre cum poţi crea un sistem electronic ce nu poate fi bruiat. La sfârşitul anului 1942, aliaţii au lansat Oboe. Acesta era un radar cu o rază de acţiune de 430 km, care calcula locul exact unde trebuiau lansate bombele şi trimitea semnale bombardierului comunicându-i aceste date, precum şi momentul propice lansării, fie noaptea, fie în timpul zilei pe vreme rea. Această tehnică era utilizată doar în zona de acţiune a radarului Oboe (pe coasta engleză) şi nu avea nicio utilitate pentru multe alte ţinte din interiorul Germaniei. Dar cel mai important era că, practic, nu putea fi bruiat. Acelaşi lucru îl vedem întâmplându-se şi azi. Cum atacurile DDOS au devenit tot mai populare (prin instrumentele DDOS uşor de folosit pe net) după anul 2000, în scurt timp au apărut şi instrumente software pentru administratorii de sistem care le confereau o mare rezistenţă la această formă de bruiere. Promptitudinea cu care au răspuns ambele părţi la armele electronice ale celuilalt în timpul celui de-al Doilea Război Mondial este tipică modului în care se desfăşoară cyber-războiul.

Marea diferenţă este că, în timpul războiului mondial, noile arme erau puse imediat în funcţiune, iar contraatacul inamicului era aşteptat cât mai curând. Deoarece nu am avut un cyber-război, cele mai bune arme noi vor fi ţinute în secret. Nu are sens să îi dai inamicului şansa de a-ţi anula noua armă înainte de a apuca să o foloseşti într-o ripostă inteligentă. Acest fapt este deosebit de important întrucât unul dintre lucrurile pe care forţele

aeriene l-au învăţat din cel de-al Doilea Război Mondial a fost semnificaţia echipamentului „alerta ameninţării”. Aceste aparate îl anunţau pe pilot că avionul său este lovit cu semnale radar. Un astfel de sistem mai sofisticat interpretează semnalele radar şi comunică pilotului dacă este vorba de unul inamic sau nu, ori tipul de radar folosit de un proiectil gata de lansare. În cazul cyber-războiului de azi, echipamentul „alerta ameninţării” este reprezentat de un număr tot mai mare de aparate pentru detectarea intruşilor pe site-urile web. Acestea te avertizează dacă cineva încearcă să pătrundă pe site-ul tău. Despre asta este vorba.

O altă lecţie reînvăţată din cel de-al Doilea Război Mondial este modul în care o mână de operatori independenţi pot deveni letali. Pe timp de noapte, într-un atac aerian asupra Germaniei din timpul războiului mondial, au fost distruse aproape toate cele 12.000 de bombardiere de numai câteva sute de avioane de luptă. Deşi erau mii de arme antiaeriene la sol, acele câteva avioane conduse de nişte piloţi talentaţi şi creativi au provocat cele mai multe pagube. Acest lucru reliefează principala diferenţă dintre atacator şi apărător în cyber-război.

Site-urile webi sunt vaste, de multe ori bine protejate (apărate împotriva hackerilor). Atacatorii, hackerii, profită de faptul că sunt o ţintă mică şi se mişcă rapid. Un hacker care este prea încet şi nu-şi dă seama că a stat prea mult pe un site bine protejat va fi capturat înainte să se poată deconecta. Dar şansele sunt de partea hackerilor, astfel încât cei mai buni dintre ei nu sunt prinşi.

De asemenea, hackerii caută să pătrundă în site-uri atunci când acestea sunt cel mai vulnerabile. Acest lucru se întâmplă de obicei când este descoperită o nouă deficienţă la serverul web. Site-urile vizate vor lua de obicei măsuri rapide pentru a remedia problema. Dar un hacker agil se va mişc a suficient de repede şi va acţiona

înainte ca acest lucru să se întâmple. Întotdeauna există site-uri ale căror măsuri de securitate sunt actualizate un pic cam lent şi de multe ori sunt atacate.

Dezvoltarea rapidă a noilor instrumente electronice şi a contraatacurilor dintre 1943 şi 1945 a fost un semn a ceea ce avea să se întâmple în cyber-război. De la al Doilea Război Mondial încoace, nu a existat o perioadă de război electronic susţinut. Dar acum suntem martorii lui pe internet. Chiar şi fără un cyber-război declanşat, lupta dintre administratorii de sistem şi hackeri generează acelaşi tip de activitate măsură/contramăsură. Mai mult, instrumentele folosite în al Doilea Război Mondial erau electronice şi trebuiau să fie create, produse, testate şi dispuse într-un aparat electronic. Deşi în cyber-război este folosit şi ceva hardware (mai ales ruterele şi firewallurile hardware), cea mai mare parte a echipamentului este formată din software. Iar aceste instrumente pot fi create, produse (scrise şi compilate), testate şi date în folosinţă în numai câteva ore. Procesul durează de obicei zile sau săptămâni, dar tot este de zece ori mai rapid decât în timpul războiului mondial şi poate dura de cel puţin o sută de ori mai puţin dacă este nevoie.

Deşi germanii au avut un mare succes în lupta aeriană din cel de-al Doilea Război Mondial (doborând 11.965 dintre bombardierele engleze care zburau noaptea), aliaţii au avut pur şi simplu mai multe aparate. Şi acest lucru evidenţiază un alt aspect al cyber-războiului. Numărul site-urilor web apărate astăzi este de ordinul milioanelor, iar configuraţia lor unică (de hardware şi software) este de ordinul miilor. Un atac cyber-războinic bine organizat şi de mare amploare ar fi dificil dacă ar doborî o mare parte dintre ele. Nu uita, internetul a fost creat pentru a supravieţui pagubelor masive. Cei mai mulţi utilizatori web ar observa un atac masiv. O mare parte dintre site-uri ar fi scoase în afara reţelei o perioadă şi totul ar merge cu viteză redusă. Dar atacatorul cyber-

războinic, precum germanii care au atacat flota aeriană masivă a aliaţilor, trebuie să provoace foarte multe pagube pentru a obţine o victorie răsunătoare. Iar site-urile web ale lumii nu sunt total nepregătite pentru atac. Cifrele contează, iar cantitatea are şi ea calitatea ei.

La începutul anului 1945, Germania era ruinată, în mare parte din cauza celor 955.000 de tone de bombe aruncate de bombardierele engleze pe timp de noapte şi a celor 623.000 de tone lansate de bombardierele americane pe timpul zilei. Ofiţerii forţelor aeriene americane care au planificat şi au condus toate acele misiuni deasupra Germaniei au venit cu idei şi perspective care au răsunat timp de 60 de ani şi formează principiile centrale ale tehnologiei şi tacticii forţelor aeriene chiar şi în prezent. Reţelele de zbor folosite deasupra Europei în anii ’40 au constituit primul cyber-război major. Dar pe vremea aceea nu era numit aşa, cu toate că folosea numai informaţii şi aparatură electronică. Bombardierele aveau nevoie în permanenţă de informaţii despre locul în care se aflau ei, ţintele lor şi aeronavele din apărarea germanilor.

Nemţii încercau să găsească bombardierele. Şi ambele părţi se străduiau să nege informaţiile celuilalt. Astăzi, ţintele nu mai sunt oraşele germane sau bombardierele care zboară. Acum avem cyber-războinici care se mişcă pe net cu viteza luminii căutând site-uri pe care să le înlăture de pe net sau informaţii pe care să le corupă sau să le fure. Spaţiul aerian a fost înlocuit de cel cibernetic, iar bombele şi armele sunt toate electronice. Dacă toate acestea induc senzaţia de déjà vu, aşa şi trebuie. Este un lucru bun, deoarece arată că, deşi cyber-războiul este înfricoşător, el nu este ceva nou. S-a mai dus şi înainte. Atunci, ca şi acum, victoria aparţine celor mai inteligenţi şi cu cele mai multe instrumente. America îndeplineşte ambele condiţii. Sigur, şi tipul cel mic poate să câştige, şi uneori chiar o face. Dar victoria este de obicei de partea „marilor batalioane”, aşa cum spunea

Napoleon. Putem fi înfrânţi dacă lenevim şi subestimăm duşmanul (oricine ar fi el). Şi nu trebuie să aşteptăm un cyber-război pentru a ne apăra. Webul se află în permanenţă într-un conflict de mici dimensiuni. Este bine pentru că ne aminteşte mereu ce se poate întâmpla dacă încetăm să ne mai apărăm.

STUDII DE CAZ DESPRE CYBER-RĂZBOI

Cyber-războiul a atras atenţia FBI în anii ’90. Iată mai jos modul în care au prezentat federalii cele trei atacuri care i-au motivat să se organizeze şi să meargă pe urma infractorilor de pe internet. Se poate citi exact textul dintr-un raport FBI.

Laboratorul din Rome al forţelor aeriene (1994)

În martie 1994, administratorii de sistem de la laboratorul din Rome – New York au descoperit că reţeaua lor este atacată. Forţele aeriene au desemnat două echipe pentru a face investigaţii. Atacurile au fost identificate la un ISP (Internet Service Provider) mai întâi în New York, apoi în Seattle, Washington, unde se termina linia (atacatorii folosiseră linii telefonice). Au urmat monitorizări la laboratorul din Rome şi au fost identificate două alianţe sau grupări de hackeri – Kuji şi Datastream Cowboy. Au fost solicitaţi informatori şi cineva a recunoscut un hacker din Regatul Unit; acesta se lăudase că spărsese diverse sisteme ale armatei americane. Statele Unite au luat apoi legătura cu Scotland Yard-ul, care a descoperit că hackerul „făcea prăpăd” din Columbia şi Chile până la New York, folosindu-se de companiile telefonice şi de ISP-ul din New York ce constituia un punct de plecare pentru atacul asupra laboratorului din Rome. Hackerul englez a fost apoi observat stabilindu-şi ţinte precum comandamentul NATO, Centrul Goddard Space Flight şi baza de forţe aeriene Wright-Patterson. Cel puţin opt ţări erau folosite ca mijloace ale acestor atacuri. Scotland Yard-ul avea destule informaţii pentru a emite un

mandat de arestare, ceea ce a şi făcut după ce au fost accesate datele de la Institutul de Cercetare Atomică din Coreea de Sud. Pe scurt, la laboratorul din Rome au fost monitorizate peste 150 de intrări frauduloase venite din o sută de puncte diferite. Conform rapoartelor, alte cel puţin o sută de victime au mai fost lovite.

Datastream Cowboy, un elev englez de 16 ani, a pledat vinovat şi a fost amendat. Mentorul său, Kuji, un tehnician israelian de 22 de ani, a fost găsit nevinovat, pentru că în Israel nu existau legi pentru astfel de incidente.

Receptorul eligibil (1997)

Receptorul eligibil a fost primul exerciţiu de război informaţional (RI) din această ţară. 35 de oameni au făcut parte din Echipa Roşie care timp de peste 90 de zile a folosit tehnologie şi software noi-nouţe. Scenariul era cu un stat tâlhar care refuza confruntarea militară directă cu SUA, în vreme ce urmărea să atace sistemele de informaţii americane vulnerabile. O parte dintre scopurile acestui stat erau să ascundă identitatea atacatorilor şi să întârzie sau să respingă orice ripostă militară din partea Statelor Unite.

Au fost realizate o serie de atacuri (toate simulate) asupra reţelelor de energie şi de comunicaţii din Oahu, Los Angeles, Colorado Springs, St. Louis, Chicago, Detroit, Washington, DC, Fayetteville şi Tampa. Deşi de încredere, rezultatele neclasificate nu au un impact prea mare; în general se crede că site-urile guvernamentale şi comerciale sunt cel mai uşor de atacat şi de înlăturat. Acest exerciţiu a servit ca un semnal de alarmă pentru mulţi. Generalul Campbell, conducătorul Joint Task Force de la Pentagon – Apărarea reţelelor computerizate, a notat că receptorul eligibil „a demonstrat clar lipsa noastră de pregătire pentru un atac cibernetic şi psihic asupra infrastructurii militare şi civile”. Apoi, purtătorul de cuvânt al Pentagonului, Kenneth Bacon, a declarat că „receptorul

eligibil a fost un important exerciţiu relevant care ne-a făcut să ne dăm seama că trebuie să ne organizăm mai bine pentru a face faţă unor posibile atacuri asupra sistemelor noastre de calculator şi asupra infrastructurii informaţionale”. Senatorul John Kyl a declarat în 1998:

„Ei bine, cyber-terorismul este surprinzător de uşor. Este greu să masori asta în cuvinte, dar au fost făcute câteva exerciţii în acest sens. Unul dintre ele, care a fost prezentat şi în mass-media, numit receptor eligibil, a demonstrat în termeni reali cât de vulnerabilă este reţeaua de transporturi, cea electrică şi altele în faţa unui atac al unor hackeri – oameni care folosesc echipament convenţional, altfel spus, nimic ieşit din comun”.

Răsăritul soarelui (1998)

În februarie 1998, mai multe reţele de la Departamentul Apărării au fost atacate folosindu-se de o vulnerabilitate bine cunoscută în sistemul de computer Solaris (bazat pe Unix). Atacatorii au testat serverele Departamentului Apărării pentru a vedea dacă există vreun punct slab; au exploatat vulnerabilitatea şi au intrat în sistem; au implantat un program de adunare a datelor; mai târziu s-au întors pentru a colecta datele.

O parte din probele iniţiale păreau că provin de la Universitatea Harvard şi din Emiratele Arabe Unite (EAU), fiind direcţionate spre Pearl Harbor şi către o parte din bazele forţelor aeriene: Kirtland, Lackland, Andrews, Columbus, Gunter şi Tyndall. Activităţile de intruziune de mai târziu au fost monitorizate din EAU, universitatea statului Utah, şi de un site web comercial pentru o parte din bazele forţelor aeriene. Ulterior s-au realizat monitorizări la zeci de alte site-uri militare americane şi universităţi. Activitatea internaţională a fost urmărită în Germania, Franţa, Israel, EAU şi Taiwan. Peste 500 de sisteme de calculator au fost compromise, inclusiv site-urile militare, comerciale şi educaţionale de către atacatori care foloseau instrumente rudimentare.

În cele din urmă, elevii de la California High School au fost arestaţi şi au pledat vinovat. Mentorul lor, un israelian de 18 ani, a fost şi el arestat şi inculpat. Cu toate că Departamentul Apărării l-a numit „cel mai bine organizat şi mai sistematizat atac de până atunci”, mulţi nu l-au luat prea în serios pentru că „Departamentul de Justiţie a susţinut că nu a fost compromisă nicio informaţie clasificată”. Nu au fost dezvăluite detalii despre ce au făcut exact hackerii.

Cu toate acestea, unii au tras nişte învăţăminte, şi anume că Răsăritul soarelui a confirmat descoperirile receptorului eligibil: sistemele de informaţii americane erau vulnerabile. Mai mult, unii susţin că diverse probleme legale au rămas nerezolvate (de exemplu, restricţiile statutare, nevoile de investigaţii competente şi problemele private care întârzie cercetările), nu există indicaţii clare şi sisteme de avertizare bine puse la punct, sistemele de detectare a intruşilor sunt insuficiente şi există prea multă birocraţie guvernamentală care întârzie un răspuns util.

Centrul pentru Protecţia Infrastructurii Naţionale Americane

KOSOVO KAPERS

În timpul Războiului din Kosovo din 1999, forţele aeriene americane au pătruns în reţelele de comunicare sârbeşti folosind sateliţi şi aeronava EC-130 Compass Call. Doreau să însereze mesaje false în sistemele sârbeşti despre raiduri aeriene inexistente şi alte atacuri. Încurajate de succesul avut şi dorind să îşi îmbunătăţească abilităţile, forţele aeriene au alocat mai multe resurse în aceste activităţi de cyber-război.

Din 1999, au fost puşi pe orbită mai mulţi sateliţi cu mai multe funcţii. Cu toate acestea, experienţa din Kosovo i-a pus pe avocaţi pe jar. Problema folosirii semnalelor de la sateliţi şi de la aeronave pentru a interfera cu sistemele de comunicare militare are şi un dezavantaj: de multe ori

este imposibil să eviţi interferarea şi cu sistemele de comunicaţii civile. Ceea ce armata numeşte „pagube colaterale” (civili loviţi din greşeală de atacuri destinate ţintelor militare) a devenit un subiect fierbinte din punct de vedere politic: unele ONG-uri (organizaţii nonguvernamentale) încearcă să înfiinţeze curţi internaţionale pentru judecarea cazurilor de infracţiune din timpul războiului. Aceasta este o problemă ce apare mai degrabă în războaiele care încă nu au fost declarate. La fel s-a întâmplat şi în Kosovo în 1999, când avioanele de război NATO au început să bombardeze pentru a-i opri pe sârbi de a-i ataca pe albanezi. A fost o situaţie obscură şi nimeni nu era sigur cine are dreptate. După ce sârbii au doborât un bombardier F-1 17 american, au fost lansate şi armele electronice. Pagubele colaterale ale civililor sârbi nu au atras atenţia mass-mediei şi nu a existat niciun titlu stânjenitor care să vorbească despre „armele electronice inumane”. Dar pericolul nu a dispărut. Începând cu 1999, cyber-războinicii au ordine să planifice operaţiuni de apărare pe care să le stabilească cu avocaţii reprezentanţi şi cu experţii în afaceri publice (controlul media asupra pagubelor). Deşi în mare parte a fost un truc al mass-media, sârbii au avut parte de ştiri pozitive făcându-şi publice propriile eforturi din cyber-război. A fost o poveste minunată pentru mass-media mondială care a produs o consternare de moment la Pentagon şi la Casa Albă, astfel încât nu a fost un efort total irosit. Reporterii străini erau invitaţi într-o încăpere plină cu elevi de liceu sârbi făcându-şi de cap pe PC-uri conectate la internet. Dar elevii erau doar amatori care foloseau instrumente ale unor script kiddies pentru a lansa atacuri inofensive.

Un grup mai important de cyber-războinici s-a mobilizat împotriva SUA atunci când Ambasada Chinei din Serbia a fost bombardată accidental. Mii de hackeri chinezi s-au mobilizat către ţinte americane, deşi, oficial, guvernul chinez nu era interesat de acest aspect. Totuşi,

nu au fost provocate pagube majore. Guvernul chinez a văzut paginile web americane distruse şi a închis site-uri web în semn de avertisment pentru SUA în privinţa ameninţării cyber-războinice din Est.

Forţele aeriene americane au privit Războiul din Kosovo ca pe o răzbunare a eforturilor lor cyber-războinice de mai înainte. Ulterior, forţele aeriene au înfiinţat organizaţii cyber-războinice pentru a accelera dezvoltarea armelor din arena războiului cibernetic. Au fost puse la punct noi şcoli şi cursuri – în acelaşi timp cu sistemul şcolar de mare amploare iniţiat deja în războiul electronic – pentru instruirea cyber-războinicilor.

Poate faptul cel mai important este că un ofiţer cyber-războinic al forţelor aeriene a fost adăugat personalului care a planificat şi a controlat operaţiunile de luptă. A fost o mişcare importantă pentru cyber-războinici, întrucât comandanţii ar fi avut întotdeauna la dispoziţie în camerele de război informaţii pertinente.

Pornind de la experienţa din Kosovo, forţele aeriene au căutat cu mai multă atenţie oportunităţile de cyber-război. Au descoperit că există mult mai multe decât s-ar fi aşteptat. De exemplu, multe naţiuni, inclusiv China, folosesc reţeaua de comunicaţii civilă pentru controlarea sistemelor de apărare aeriană (şi comunicaţiile militare în general). Naţiunile mai înstărite construiesc sisteme de comunicare militare separate, mai puţin vulnerabile. Sistemele de comunicaţii civile sunt construite cu componente noi-nouţe şi pe baza principiilor cunoscute (pentru a menţine costurile mici, este o afacere competitivă). Aceasta a făcut ca planificarea şi executarea atacurilor cibernetice să fie mai uşor de realizat pe aceste sisteme. În plus, există o mare diferenţă între atacul cibernetic asupra comunicaţiilor inamice şi un atac electronic. Cyber-războinicii nu vor doar să prăbuşească un sistem, aşa cum ar vrea cei din războiul electronic. Nu, ei vor să deţină o parte din controlul asupra comunicaţiilor

inamice. Astfel te poţi juca cu mesajele inamicului, aşa cum a fost în Kosovo. Implantarea informaţiilor false şi derutante este mult mai valoroasă decât blocarea comunicaţiilor electronice inamice (lucru care este util, dar duşmanul va găsi totuşi un alt mod de comunicare, poate mai puţin eficient). Există avantaje în sistemul de comunicare civil, mai ales unul aşa de mare precum cel din China (care serveşte mai mult de un sfert de miliard de clienţi). Aceste sisteme sunt aproape imposibil de distrus. Poţi avaria părţi importante din ele, dar, la fel ca internetul, sistemele de comunicare moderne sunt construite pentru a încasa lovituri şi a rezista.

RĂZBOIUL ELECTRONIC PESTE BALCANI

SUA deţin un transmiţător radio-TV numit Commando Solo (aeronava EC-130E, un C130 special echipat). A fost folosit cu adevărat în timpul Războiului din Kosovo din 1999, dar nu s-a descurcat prea bine din cauza terenului deluros din Balcani. Totuşi, ideea de bază a acestuia a avut un răsunet destul de mare. Distruge transmiţătoarele radio şi TV ale inamicului şi apoi trimite avionul pentru a implanta mesajul pe frecvenţele cu care erau obişnuiţi localnicii. O altă aeronavă C-130 specializată, EC-130H Compass Call, s-a descurcat mai bine: scopul său era să absoarbă şi să depisteze transmisiunile electronice ale inamicului. Şi această pasăre putea să cânte şi era mijlocul prin care erau implantate mesajele false în sistemul sârb de comunicaţii al apărării aeriene.

Totuşi, defectul lui EC-130H este faptul că, fiind o aeronavă de mari dimensiuni, înceată, trebuie să se apropie destul de mult (la aproximativ o sută de kilometri) de transmiţătoarele inamice pentru a funcţiona. Dar simpla prezenţă a acestei noi forţe îi determină pe operatorii apărării aeriene şi pe comandanţi să fie mai puţin siguri pe ei şi aceasta este o mică victorie.

RAPORTUL KEYS

După Războiul din Kosovo din 1999, generalul-maior al forţelor aeriene, Ronald Keys (unul dintre ofiţerii superiori care au dirijat operaţiunile aeriene), a pregătit un raport despre ce s-a petrecut în timpul războiului informaţional din Kosovo. Interesant este faptul că superiorii lui Keys au spus că raportul nu reprezintă punctul de vedere oficial al forţelor aeriene americane, ci numai al generalului. Era o mişcare de război informaţional interesantă (însemnând că forţele aeriene voiau să facă publice informaţiile din raport, dar nu doreau să fie prezentate ca materiale oficiale). Raportul Keys a rămas neclasificat şi a tras nişte concluzii dure despre cât de victorioase şi (chiar mai important decât atât) nevictorioase sunt eforturile tuturor într-un război informaţional. Una dintre ţintele principale ale acestui raport a fost Congresul SUA, care trebuia să furnizeze banii pe care forţele aeriene îi doreau pentru a creşte randamentul războiului informaţional. De asemenea, raportul Keys a arătat numărul mare de elemente incluse în conceptul de război informaţional. Din punctul său de vedere, acesta acoperă modul în care se dirijează şi se aleg informaţiile care sunt transmise mediei, dar şi compromiterea sistemelor de comunicaţii inamice. Deşi raportul vorbea despre eforturile „NATO din războiul informaţional”, acesta aborda, în cea mai mare parte, operaţiunile americane din războiul informaţional şi cyber-război. Keys a concluzionat că NATO este mai bine pregătită din punct de vedere tehnic (având o gamă largă de instrumente şi capacităţi disponibile) decât din cel al utilizării armelor („aspectele tactice”).

Sârbii (reprezentând ce mai rămăsese din Iugoslavia) aveau mult mai puţin echipament pentru un război informaţional pe care să îl folosească, aşa că au fost nevoiţi să se descurce cu ce aveau: o lungă istorie de

folosire a înşelătoriei pentru a-i păcăli pe inamicii mai puternici, în ciuda tuturor senzorilor electronici americani (în avioane şi sateliţi), a fotografierii ziua şi noaptea şi a preluării oricărei transmisii de pe teritoriul sârb, sârbii s-au descurcat folosind o gamă largă de instrumente cu tehnologie mai puţin avansată. La sol, trupele lor ştiau cum să se ascundă, atât ei, cât şi vehiculele lor. Chiar şi cu toată supravegherea americană, tot se puteau mişca în teritoriu. Foloseau capcane şi vehicule false pe care americanii le ocheau şi le bombardau. Sârbii au subliniat cazurile când bombele inteligente au lovit ţinte civile. S-au jucat cu sentimentele americanilor la adresa victimelor nevinovate până acolo încât au început să pozeze ei înşişi în victime. Sârbii au avut succes cu „victimele civile", întrucât multe dintre naţiunile membre NATO au insistat ca ţintele bombardierelor americane să fie revizuite şi de multe ori şi-au exercitat dreptul de veto. Aceasta a redus eficienţa bombardamentelor NATO, întrucât, până era aprobarea primită, ţintele mobile se deplasau şi scăpau. De asemenea, sârbii au iniţiat un joc informaţional răutăcios, punând în circulaţie zvonuri adevărate sau false, creând confuzie şi băgând zâzanie printre membrii NATO. Sârbii erau destul de buni în războiul relaţiilor publice, în vreme ce NATO nu a reuşit niciodată să înscrie prea multe puncte în această zonă.

Gama largă de instrumente pentru războiul informaţional de care dispunea NATO a reprezentat un rateu din multe puncte de vedere. Toate informaţiile vizuale şi electronice adunate de aeronave, sateliţi şi staţii de la sol au invadat sediile centrale ale NATO, copleşind personalul şi comandanţii. Informaţiile-cheie se pierdeau de multe ori în mulţimea de date. Uneori erau identificate elemente utile, dar există bănuiala că multe informaţii valoroase nu au fost găsite niciodată. Sistemul de comunicare s-a transformat într-un blestem pentru comandanţi.

Pentru generalii americani însemna că pot primi un telefon de la preşedinte în orice moment. Cum preşedintele putea ajunge primul la personalul responsabil de sateliţi, generalul nu putea decât să tacă în timp ce şeful său de la Casa Albă îi spunea ce şi cum să facă.

Generalul Keys a concluzionat că trebuie să existe o modalitate mai bună de a face faţă avalanşei de informaţii şi managementului acestora. Din păcate, această plângere a fost auzită mereu din anii ’70 încoace. Cu toate acestea, problema pare să fi fost abordată în timpul Războiului din Afganistan din 2001.

SINDROMUL BALCANIC

De multe ori, internetul furnizează punctul de plecare pentru ambuscade cyber-războinice la care nimeni nu se aşteaptă. La începutul anului 2001, mass-media italiană a preluat un element neconcretizat de pe internet şi a publicat o poveste bizară, dar cu impact, despre susţinători ai păcii italieni care mor de leucemie ca parte a „sindromului balcanic”. Jumătate de duzină de trupe italiene muriseră din cauza bolii, apoi alte două duzini de soldaţi italieni (din cei 60.000 care au slujit în Balcani din 1995) au contractat alte boli similare. Motivul oferit a fost uraniul sărăcit. Săptămâni la rând, presa italiană şi apoi cea europeană au dezbătut povestea. Se pare că nimeni nu s-a deranjat să verifice informaţia cu doctori şi oameni de ştiinţă care aveau cunoştinţe despre acest subiect.

Uraniul sărăcit – mai dens şi mai greu decât alte metale – este folosit pentru a străpunge tancurile atunci când sunt lovite de proiectilele de 30 mm care, de obicei, sunt purtate de aeronavele A-10, la fel ca şi de armele de tanc de 120 mm. Avioanele A-10 americane au tras aproximativ 30.000 de obuze de 30 mm în Kosovo. Nu numai că uraniul sărăcit perforează blindajul, dar ia foc atunci când loveşte cu viteză mare (o milă pe secundă). Astfel cresc pagubele provocate tancului. Dar atunci când

arde, uraniul sărăcit se fărâmiţează. Cercetătorii italieni spun că aceste fragmente, care emit raze alfa, sunt cauza problemelor provocate de sindromul balcanic.

Uraniul sărăcit a înlocuit wolframul, un alt metal greu (nonreactiv) folosit pentru perforarea blindajului. Wolframul poate crea şi probleme de sănătate dacă este inhalat sau înghiţit, la fel ca şi un alt metal greu, mult mai cunoscut: plumbul.

Uraniul sărăcit este ceea ce rămâne după ce U-235, care este foarte reactiv, este înlăturat pentru a fi folosit pe post de combustibil nuclear sau pentru bombele atomice; U-235 emite radiaţii gama (sau altele) periculoase. U-238 este ceea ce rămâne, dar, deşi este încă radioactiv, emite mult mai puţine radiaţii alfa periculoase. Astfel, mult mai puţin radioactiv decât iniţial, uraniul sărăcit nu este mult mai periculos decât multe alte roci. Mii de soldaţi americani şi civili au mânuit uraniu sărăcit în ultima jumătate de secol, fără o agravare semnificativă a problemelor de sănătate. Mai mult, nu s-a înregistrat nicio creştere a cazurilor de cancer în rândul populaţiei civile din Kosovo din 1999 încoace. Specialiştii subliniază că perioada de dezvoltare a leucemiei provocate de expunerea la radiaţii durează între cinci şi zece ani. Trupele italiene au stat în Kosovo numai trei ani. Specialiştii în medicină nucleară reliefează, de asemenea, că razele alfa emise de uraniul sărăcit sunt blocate de piele. Leucemia este un cancer al măduvei spinării la care razele alfa radiate de uraniul sărăcit nu ar putea ajunge.

A existat o creştere a cazurilor de cancer în Kuweit şi Irak începând cu Războiul din Golf din 1991. Zona a fost supusă, timp de mai multe săptămâni, unor incendii ale câmpurilor petrolifere. Fumul emanat este cancerigen şi a fost mult mai abundent decât rămăşiţele obuzelor de uraniu sărăcit. Mai mult, miile de vehicule blindate care au devastat deşertul virgin au creat un nor de praf fără precedent (chiar şi pentru Arabia), care conţinea un nisip

foarte fin, asemănător talcului. Medicii locali nu au fost surprinşi de creşterea numărului de îmbolnăviri, pentru că ştiau din experienţă ce pot face fumul de petrol şi nisipul.

Aşadar, ce a făcut ca povestea cu uraniul sărăcit să fie credibilă în Italia şi în toată Europa? Un rol important l-a avut entuziasmul mass-mediei de a da curs unei istorii înfricoşătoare. De asemenea, în Italia exista o mare nemulţumire publică cu privire la acţiunile NATO din Balcani. Italia, în mod special, a fost destinaţia multor refugiaţi albanezi, veniţi atât din Albania, cât şi din Kosovo. Majoritatea atacurilor aeriene împotriva Serbiei şi Kosovo veneau dinspre bazele aeriene italiene. În timpul campaniei aeriene, atunci când s-a raportat că avioanele de război care se retrag îşi vor arunca bombele în Marea Adriatică (nu doreau să rişte să aterizeze cu ele), italienii s-au înfuriat. Deşi nu erau armate, bombele prezentau un mare risc de explozie şi un pericol real pentru pescarii italieni.

Şi internetul a avut un rol în nemulţumirea italienilor legată de implicarea în Balcani. Povestea cu uraniul sărăcit a devenit ştire pentru prima dată după Războiul din Golf din 1991 ca încă o formă de propagandă irakiană. Ar fi fost uşor dată uitării dacă nu ar fi fost stocată pe web şi reluată rapid prin motoarele de căutare. A devenit de asemenea un punct de discuţie pro-Irak/anti SUA înainte ca mass-media italiană să decidă să o preia – cu o mulţime de materiale adiacente uşor de accesat.

Acesta este războiul informaţional. Politicienii italieni ştiau că alierea cu NATO în atacarea Serbiei şi preluarea Kosovo nu va fi aprobată de popor. Invazia refugiaţilor s-ar fi îndreptat direct spre Italia, crescând numărul populaţiei de refugiaţi care era deja impopular în rândul votanţilor italieni. Ce mod mai bun de a para aceste probleme decât să te ascunzi în spatele sindromului balcanic? Mai mult, adevărata poveste a sfârşitului războiului, despre veterani cu boli fizice şi psihologice suplimentare, nu va avea prea

multă trecere, deşi adevărata natură a uraniului sărăcit va eroda, în cele din urmă, ştirea despre sindromul balcanic, în final, politicienii nu vor fi legaţi de implicarea lor în susţinerea mâniei publice cu privire la un război dus cu informaţii false.

SPAIMA Y2K

Departamentul Apărării a închis multe site-uri web militare în weekendul liber de Anul Nou 2000. Asta pentru a evita expunerea lor în faţa unor atacuri din partea hackerilor care ar fi putut găsi o deficienţă la Y2K, ce putea fi exploatată numai când ceasul trecea de la anul 1999 la 2000. Nu s-a întâmplat nimic.

Situaţia Y2K (denumirea tocilarilor pentru „Anul 2000”) a fost transformată într-o spaimă majoră de către mass-media neştiutoare şi de câteva companii de software lacome. Problema a apărut în anii ’50, când a fost dezvoltat primul software comercial. Conform standardelor de azi, existau computere micuţe, cu o memorie de numai câteva mii de biţi cu care te puteai juca. De vreme ce spaţiul era atât de restrâns, a devenit ceva obişnuit să ţii evidenţa datelor anului folosind numai ultimii doi biţi (1957 a devenit 57). Toată lumea ştia la vremea respectivă că în cele din urmă, în anul 2000, aceste două cifre vor deveni o problemă (computerul nu avea să ştie dacă este vorba despre 1900 sau 2000). De fapt, problema avea să se ivească chiar mai devreme. Multe firme comerciale erau nevoite să facă planificări în avans şi să folosească date viitoare. Gândeşte-te la o bancă ce ţine pe computere evidenţa a 30 de ani de ipoteci. Un astfel de software trebuia să fie gata pentru Y2K încă de la sfârşitul anilor ’60.

Primii programatori au presupus că programele pe care le creează vor fi înlocuite cu altele care să folosească patru cifre pentru scrierea anului înainte de 2000. Ei bine, nu s-a întâmplat aşa. Multe dintre primele programe

software nu au fost înlocuite. Au fost, pur şi simplu, actualizate astfel încât să poată funcţiona pe computere mai noi şi mai puternice. Regula de bază era „dacă nu e stricat, nu repara”. Dar cum anul 2000 se apropia, era evident că aveau să sufere consecinţele. Problema majoră era că nimeni nu ştia exact unde sunt problemele şi cât de multe sunt. Aceasta a făcut mass-media să îşi închipuie cele mai rele scenarii (senzaţionalul vinde mai multe ziare) şi imediat au apărut numeroşi consultanţi de software pentru a-i asista pe managerii impacientaţi în privinţa rezolvării problemei.

FUD (Fear, Uncertainty, Doubt) 1 a provocat mai multă agitaţie decât se prevăzuse. Până la urmă, managerii de software au făcut rost de banii necesari pentru actualizarea unei părţi mari din vechile coduri. Până în anii ’80, cele mai noi programe erau făcute cu date ce foloseau patru cifre pentru exprimarea anului. Majoritatea băncilor şi instituţiilor financiare au avut de-a face cu problema Y2K încă din anii ’70. Dar programele care necesitau cea mai mare atenţie erau scrise în coduri cu adevărat vechi în limbaje de calculator (precum COBOL) pe care nu le mai folosea aproape nimeni. Mulţi programatori pensionaţi au fost plătiţi cu sume mari pentru a părăsi terenul de golf şi a-şi relua munca.

Ceea ce îi îngrijora cel mai mult pe oameni erau chestiunile foarte importante care ar fi putut merge prost din cauza problemei Y2K. în decembrie 1999, Departamentul Apărării a anunţat că cele 2.101 de computere esenţiale pentru conducerea armatei SUA erau deja pregătite pentru Y2K şi alte 5.488 (minus zece) de computere „destul de importante” erau şi ele gata.

Dar teama de problemele majore cauzate de Y2K în Europa de Est a determinat Departamentul Apărării american să evacueze 352 de diplomaţi (şi subordonaţii lor) din ambasadele SUA şi consulatele din Rusia, Belarus, Moldova şi Ucraina. De asemenea, americanii au plătit

pentru aducerea unor experţi ruşi în America (şi au trimis americani în Rusia) pentru a supraveghea centrele de comandă la trecerea în anul 2000. Exista teama (în majoritatea cazurilor nefondată) că ceva ar putea merge prost cu rachetele nucleare sau cu sateliţii spaţiali.

Unele lucruri chiar au mers prost. Departamentul Apărării a numit situaţia „un incident serios”: un satelit american spion (o rachetă Keyhole) a pierdut aproape trei ore de date atunci când staţia de la sol a avut o problemă Y2K. Asta a fost tot, cel puţin în ceea ce priveşte problemele majore.

Au fost consemnate şi probleme mai mici. O maşină de înregistrare de la un PX din Okinawa a fost scoasă din funcţiune pentru o vreme din cauza problemelor Y2K. O parte din computerele care fuseseră „aranjate” au afişat anul 1900 în loc de 2000. Au existat situaţii similare la multe centrale electrice nucleare (de unde, de obicei, nu se raportează prea multe), dar nu a fost nimic atât de grav încât să fie necesară întreruperea operaţiunilor.

Armata a fost atât de uşurată, încât i-a recompensat cu medalia „Servicii merituoase” pe managerii de proiect care au depus eforturi pentru ca miile de sisteme ale computerelor militare să fie pregătite pentru Y2K. Aceia care au petrecut cel puţin un an la problemele Y2K au primit medalia „Onor militar”. Pentru a recompensa sutele de trupe care în ultimele câteva luni depuseseră eforturi mari, toţi cei care lucraseră cel puţin două luni la Y2K şi se remarcaseră au primit medalia

„Realizare militară”. Alţii care au luat parte la proiectele Y2K au primit certificate sau monede-suvenir care să arate că au servit unei operaţiuni de mare amploare şi mai ales de succes.

Deşi în mare parte a fost doar o înşelătorie, niciunul dintre profesioniştii în software nu s-a plâns cu voce tare. Aceşti oameni au dat curs farsei pentru că până la urmă primeau bani pentru repararea unei părţi din software-ul

învechit. A fost o mare controversă, chiar dacă nevăzută (de public), între profesioniştii în software (programatorii şi superiorii lor) şi conducere timp de mai multe decenii. Odată ce a fost limpede că software-ul din anii ’50 şi 60 nu va fi înlocuit sau actualizat în întregime, comunitatea din domeniu a ştiut că vor apărea probleme serioase. În anii ’60, acestea au început să iasă la suprafaţă. Pionierii care creaseră aceste software-uri începuseră să iasă la pensie, iar managerii lor au continuat să păstreze legătura cu ei (majoritatea programatorilor erau şi încă mai sunt în general bărbaţi). Chiar şi înainte de criza Y2K, programatorii pensionaţi erau chemaţi înapoi (pentru contracte de consiliere) pentru a repara software-urile vechi pe care noii programatori nu le puteau înţelege prea bine. De fapt, Ziua Recunoştinţei a fost amânată până la sfârşitul Războiului Rece. Rusia era una dintre marile naţiuni care încă mai folosea vechile limbaje de calculator, fapt ce a dus la angajarea mai multor persoane pentru întreţinerea vechiului cod. Dar numărul semnificativ de programatori ruşi din companiile americane a provocat alte temeri în privinţa eforturilor pentru Y2K. A fost evidenţiat faptul că toţi acei angajaţi temporar care au fost aduşi pentru a săpa prin software-ul vechi pentru a căuta şi rezolva problema scrierii anilor cu două cifre, pe lângă acest lucru puteau adăuga un cod care să le permită ulterior accesul în sistemele în care rulau aceste programe. Această problemă s-a pus mai ales în cazul guvernului şi al sistemelor bancare. Au existat multe cazuri suspecte, dar numai câteva astfel de întâmplări au avut loc. Această teamă era mai mult o ultimă suflare a celei provocate de Y2K. În primul rând, majoritatea programelor cărora trebuia să li se acorde atenţie în privinţa Y2K nu erau conectate la internet sau la vreun alt tip de reţea. Dar acelea care erau, de obicei erau verificate de personalul obişnuit sau de subcontractanţii de încredere. Totuşi, niciodată nu poţi fi sigur.

COD ROŞU PENTRU CHINA

Războiul informaţional a lovit cu putere în iulie 2001, când mii de site-uri web au fost atacate de virusul numit Code Red (Codul roşu). La început, nimeni nu a ştiut de unde vine acest virus, cu toate că, atunci când lovea un server web vulnerabil (un PC care rula un site web), schimba site-ul cu o pagină pe care scria „Hăcuit de chinezi”. Codul roşu a fost un exemplu despre cum poate fi dus un război informaţional, în primul rând, acest virus opera din cauza unei deficienţe în software-ul Microsoft al serverului web. Pe 18 iunie, Microsoft a emis un buletin de securitate despre vulnerabilitatea acelui software şi furniza şi o remediere. Dar prin anunţarea acestei probleme, Microsoft a dat de ştire băieţilor răi că există un mod de a pătrunde pe servere şi a provoca pagube. Pe 13 iulie, au fost primite primele rapoarte ale virusului Code Red. Acesta a fost rapid înlăturat şi s-a descoperit că are o serie de caracteristici interesante. În primul rând, opera exclusiv în memorie, fără să lase nimic pe hard drive. Acest lucru îl făcea mai greu de găsit, cu toate că desfigura paginile web ale serverelor. În al doilea rând, începea imediat să apeleze alte servere, alese aleatoriu în căutarea celor vulnerabile, pentru a le infesta. La vremea respectivă existau aproximativ 3, 5 milioane de servere care prezentau riscul de a fi atacate (21 de procente din cele 17 milioane de servere active care rulau software Microsoft). S-a estimat că virusul Code Red poate infesta jumătate de milion de servere în 24 de ore. Concret, numai 300.000 au fost afectate. Asta deoarece căutarea nu era aleatorie în totalitate, o funcţie putând furniza autorilor Code Red o listă mare cu serverele vulnerabile. Dar la o săptămână după apariţia primului Code Red, a apărut o variantă modificată care mergea după fiecare server la care putea ajunge. Nu se ştie dacă fiecare server vulnerabil a fost lovit sau ce procent din serverele

Microsoft au fost reparate pentru a ţine virusul la distanţă. Dacă un administrator de server repara pur şi simplu paginile web distruse şi nu reseta serverul PC-ului, Code Red intra în hibernare şi devenea din nou activ în anumite zile ale lunii, fie pentru a încerca să se răspândească, fie pentru a executa o negare a atacului asupra serverului Casei Albe americane. Acest lucru a fost evitat prin schimbarea adresei IP a serverului Casei Albe şi eliminarea datelor inutile care se duceau la vechea adresă. Se pare că armata SUA se simţea vulnerabilă, întrucât şi-a închis o mare parte din site-urile web timp de mai multe zile, pentru a se asigura că serverele sunt reparate şi pentru a ţine virusul la distanţă.

O particularitate a Code Red a fost că nu avea nimic special. Programele de tip vierme, precum Code Red, sunt cunoscute ca fiind rapide. Code Red era periculos din cauza accesului foarte uşor pe care îl furniza serverul defect al software-ului Microsoft. „Vulnerabilitatea Index Server ISAPI” pe care a exploatat-o virusul era doar una dintre cele multe ale software-ului. Se ştie că serverul software-ului Microsoft este plin de deficienţe, fiind descoperită cam o vulnerabilitate pe lună (şi 40 de deficienţe de toate felurile în cele şapte luni care au precedat atacul Code Red). Încercările de a face Microsoftul mai ferm în privinţa securităţii sistemului au un succes limitat. Între timp, originalul Code Red hiberna pe servere acolo unde nu era detectat. Aceste site-uri Code Red au fost reactivate la ora 20, pe 31 iulie 2001. Dar al doilea val s-a dovedit mai puţin răvăşitor decât primul. Între timp, erau lansate versiuni mutant ale virusului. Existau aproximativ un milion de servere care erau încă vulnerabile la sfârşitul lunii iulie şi puteau fi transformate în maşini de spamuri care să asfixieze netul atunci când avea să lovească al doilea val. Dar site-urile care sunt cel mai atent urmărite (guvernamentale şi comerciale) au reuşit să se apere.

Guvernul american este unul dintre clienţii fideli ai produselor Microsoft, în mare parte pentru că sunt uşor de folosit. Acest lucru este important pentru că guvernul nu poate concura cu sectorul comercial atunci când vine vorba despre angajarea celui mai priceput în ale calculatoarelor, într-un cyber-război viitor vor fi folosite programe precum Code Red pentru că toate serverele care folosesc software Microsoft nu vor fi reparate. Ei bine, cel puţin nu până când va fi lansată o nouă versiune a software-ului şi toate serverele vor fi actualizate. Altfel spus, mulţi ani de aici înainte, naţiunile ostile vor avea acces la o parte din serverele americane. Versiunile de război ale Code Red nu vor distruge paginile web şi nu îşi vor face simţită prezenţa. Nu, acea versiune va sta ascunsă până când va primi comanda să lanseze o dezminţire a atacului sau o altă înşelătorie pe serverele americane.

Se pune întrebarea dacă Microsoft va fi vreodată judecat pentru înaltă trădare.

Viermele Code Red a fost descris ca fiind software-ul media perfect. Nu provoacă multe pagube, deşi o formă mutantă ar fi letală şi va exista latent ani în şir (până când toate serverele care rulează NT sau Windows 2000 vor fi actualizate sau reparate). Dacă nu ai prea avut parte de ştiri azi, Code Red va fi întotdeauna acolo pentru un alt titlu înspăimântător. Dar acest virus a adus şi un serviciu publicului, făcând tot mai mulţi oameni (mai ales administratorii de sistem neştiutori) să fie conştienţi de importanţa actualizării software-ului. Un alt efect secundar a fost sublinierea importanţei aducerii unor schimbări fundamentale în modul de operare al internetului. Încă de la început, a fost foarte uşor pentru utilizatori să îşi ascundă identitatea pe internet. Nimeni nu a prevăzut creşterea imensă şi comercializarea pe care acesta le-a avut. Aşadar, la început, securitatea nu era o problemă importantă. Este evident că acest lucru s-a schimbat. Reconfigurarea internetului pentru a elimina anonimatul

ar fi un risc major, cu atât mai dificil cu cât ar apărea abandonul din partea oamenilor. S-a propus asta de mai multe ori. Dar dacă totul ar putea fi depistat, nu înseamnă că acesta ar fi leacul, întrucât întotdeauna vor exista alternative. Dar îngreunarea lucrurilor pentru hackerii black hat este bine-venită.

Un studiu din august 2001 al guvernului SUA a concluzionat că viermele Code Red a venit probabil dintr-o universitate din Guangdong, China. O organizaţie de cercetare nonguvernamentală, Computer Economics, a estimat că sumele pentru repararea pagubelor produse de Code Red se ridică la 2,6 miliarde de dolari (1,1 miliarde de dolari pentru inspectarea şi curăţarea serverelor şi 1, 5 se regăsesc în productivitatea pierdută cât timp serverele nu au funcţionat). Această afirmaţie se baza pe estimarea conform căreia aproximativ un milion de servere au fost infestate.

CAPITOLUL 5
CYBER-RĂZBOAIE ACTUALE ŞI VIITOARE

TERMENI TEHNICI

Glosarul complet, ce include şi termenii definiţi mai jos, poate fi găsit la sfârşitul cărţii.

Crackerii sunt hackeri puşi pe rele. Aceşti vandali ai internetului mai sunt numiţi şi hackeri black hat1.

Asta pentru a-i diferenţia de hackerii buni, care sunt cunoscuţi sub numele de hackeri white hat2. Practic, internetul a fost construit de o mulţime de hackeri (programatori care analizează o problemă a software-ului până o rezolvă. Aceasta se numeşte „analiză bună”).

Criptarea se referă la utilizarea codurilor pentru a face ca e-mailul sau datele tale să fie dificil (sau imposibil) de folosit. Criptarea există de mii de ani şi încă mai

foloseşte acelaşi principiu de bază al substituirii celor scrise de tine cu alte litere sau cifre. Oricine are cheia decriptării (care arată ce trebuie înlocuit în materialul codat pentru a-l transforma din nou în ceva ce poate fi înţeles) poate citi materialul codat. Computerele au schimbat metoda criptării. Unul dintre primele computere moderne a fost inventat în cel de-al Doilea Război Mondial pentru a decripta codurile germanilor. Încă de pe atunci computerele au fost folosite pentru criptarea şi decriptarea (prin folosirea cheii) mesajelor codate. Teoretic, este posibil să foloseşti un computer pentru a decripta un mesaj codat fără să utilizezi cheia. Dar pentru asta este nevoie de mult timp. În funcţie de cât de puternic este codul criptat, o astfel de „decriptare forţată" este, la urma urmei, din motive practice, imposibilă.

Chiar acum au loc mai multe cyber-războaie şi alte câteva sunt gata să izbucnească.

CYBER-RĂZBOIUL ESTE PRINTRE NOI

Ideea de cyber-război nu a fost încă luată în serios de mulţi oameni, în general, oamenii îşi închipuie hackeri şi câţiva cyber-criminali. Dar an după an, tot mai mulţi utilizatori de internet se confruntă personal cu cyber-războiul. De multe ori, asta înseamnă doar infestarea computerului cu un virus sau închiderea reţelei de la birou pentru câteva ore sau zile, pentru rezolvarea problemelor cauzate de cyber-terorism. Dar este această problemă suficient de gravă pentru a începe cursa pentru securitatea webului? Există semne că ar fi. În anul 2000, când China şi Taiwan se certau pentru independenţa taiwaneză, paginile web pro-Taiwan erau distruse în mod regulat. Inculpaţii au fost identificaţi ca provenind de pe serverele din Beijing.

O activitate similară a avut loc atunci când serverele Departamentului Apărării au fost invadate. Vinovaţii operau de la Moscova. Când DOD i-a denunţat, ruşii au răspuns că nu ar fi atât de neîndemânatici încât să fie

prinşi în cazul în care chiar ar fi vinovaţi. Ei au dat vina pe amatorii în căutare de senzaţii tari. Poate că au existat şi aceştia, întrucât multe dintre atacuri au fost făcute cu instrumente şi tehnici nu prea avansate. Dar atacurile ruşilor aveau loc numai între orele 9 şi 5 (ora locală) şi niciodată în timpul vacanţelor ruseşti. Angajaţii guvernului lasă întotdeauna urme. Cei pe cont propriu lucrează de obicei la ore diferite, de multe ori în timpul nopţii (ora locală). În timpul Războiului din Kosovo din 1999, sârbii nu au ţinut secret faptul că au mobilizat crackerii locali pentru a riposta. Au existat şi ceva înşelătorii, dar fără pagube majore. Iar aceşti hackeri voluntari sârbi lucrau la orice oră.

Oricine ar fi cel care a iniţiat hackingul, atât ruşii, hackerii, cât şi restul lumii ştiau un lucru: America este cea mai vulnerabilă naţiune când vine vorba despre cyber-război. Americanii sunt în fruntea clasamentului în privinţa postării unor servicii esenţiale şi a unor operaţiuni comerciale pe internet. De multe ori, acesta este un avantaj pentru personal, astfel încât, atunci când este o urgenţă, cei responsabili se pot pur şi simplu loga pe site-ul web al companiei şi rezolva problema. Să luăm ca exemplu un sistem al unui rezervor de apă. Dacă pe timpul weekendului apare vreo problemă, inginerul poate fi alertat acasă. Acesta se poate loga la site-ul sistemului rezervorului, verifică starea digurilor şi cursul apei (prin senzori şi comenzi postate pe internet) şi face ajustările, fără să fie nevoie să bată tot drumul până la dig. Un alt beneficiu al acestui aspect este că mai mulţi experţi se pot conecta în acelaşi timp, pot examina datele, discuta situaţia cu ajutorul unui chat room sau printr-o conferinţă, după care pot lua măsurile impuse. Acelaşi sistem se aplică şi fabricilor, laboratoarelor de cercetare sau clădirilor cu birouri impozante. Dezavantajul este că, dacă vreuna dintre aceste facilităţi nu dispune de o securitate adecvată a conexiunilor la internet, sistemul lor poate fi

spart şi se pot provoca multe pagube. Se poate întâmpla ceva grav, precum deschiderea unui dig pentru a da drumul la toată apa sau manipularea comenzilor unei fabrici cu scopul de a provoca o explozie sau alte pagube.

Se ştie acum că informaţia este o sursă importantă de putere, iar cantităţi tot mai mari de date, mai ales militare, sunt online. Din fericire, cei mai mulţi experţi în internet din lume sunt americani. Şi apoi, există şi tendinţa ca în situaţii de criză să se adune toţi şi să nu se lase până nu rezolvă problemele. Nu subestima acest lucru, întrucât este motivul principal pentru care SUA au câştigat Războiul Rece, ca să nu mai spun de al Doilea Război Mondial, cursa spaţială ş.a.m.d. Oricine ar lansa un atac asupra facilităţilor americane comerciale sau militare s-ar trezi pe cap cu unii dintre cei mai talentaţi oameni specializaţi în internet de pe planetă. Până acum, atacurile asupra digurilor, fabricilor sau bazelor de date americane au fost în mare parte doar teoretice. Site-urile Departamentului Apărării ce conţin informaţii militare se află sub atac de mai bine de un deceniu, iar o parte dintre acestea au ajuns subiect de ştiri. Acest război este în continuă desfăşurare, chiar dacă în mare parte are loc departe de privirile publicului. Din când în când, mai ies totuşi la suprafaţă unele aspecte. Ştim că Departamentul Apărării îşi îmbunătăţeşte în permanenţă apărarea, iar companiile care folosesc foarte mult internetul încearcă şi ele în mod constant să fie cât mai puţin vulnerabile.

ATACURI CIBERNETICE ASUPRA DEPARTAMENTULUI APĂRĂRII AL SUA

Sistemele computerelor de la Departamentul Apărării al SUA au fost tot mai des ţinta atacurilor cyber-războinice din toate părţile. Totul a început în anii ’80, pe măsură ce tot mai mulţi oameni au avut acces la internet. Cunoscutul film din 1984 *Wargames* a încurajat această tendinţă. Filmul prezenta un hacker adolescent care intra în sisteme

ce nu existau; şi aproape (doar în film) a lansat atacuri nucleare. Mulţi dintre tineri nu au realizat că filmul era doar ficţiune, iar încercările de a „sparge Pentagonul” au devenit în toată lumea un fel de sport de sală. În ultimii ani, atacurile asupra site-urilor Departamentului Apărării au devenit tot mai distructive şi se pare că exerciţiile de instruire pentru hackerii străini pregătesc un război major. Numărul atacurilor a crescut în mod constant începând cu anii ’90.

Atacuri anuale asupra Departamentului Apărării
Anul Atacuri pe net

Acestea sunt doar atacurile care au fost înregistrate. Cele mai periculoase nu sunt detectate şi nimeni nu ştie cum şi de ce au avut loc. Foarte puţine atacuri de acest fel provoacă pagube majore. De exemplu, în 2001, la fiecare o mie de încercări de atac asupra armatei, 6, 69 au avut succes. În 2000 au avut loc 11, 6 intrări frauduloase la fiecare o mie de încercări. Foarte puţine dintre acestea au fost serioase, pentru că cele mai importante computere militare sunt de obicei mai bine protejate. Dar evident că există riscuri. Cu toate acestea, experţii în internet ai armatei au consemnat că 98% din spargerile reuşite au fost rezultatul faptului că hackerii au profitat de slăbiciunile de care ştiau şi care puteau sau ar fi trebuit reparate.

Atacurile au scăzut semnificativ după 11 septembrie 2001 şi datorită faptului că majoritatea reţelelor militare au fost retrase de pe internet pentru o vreme. Armata menţine de asemenea reţele independente de internet. Până la sfârşitul anului, atacurile asupra reţelelor militare americane crescuseră foarte mult chiar, rămânând totuşi la o rată anuală de 40.000. Pe viitor e posibil să fie mai multe atacuri, dacă numărul acestora continuă să crească de la zi la zi. În primii ani, probabil că numărul lor a fost declarat mai mic, întrucât multe dintre cele ratate (sau chiar

reuşite) au trecut neobservate. Tehnologia de apărare mai avansată (detectori de intruziune şi sisteme de monitorizare) detectează tot mai multe încercări şi le opreşte pe multe dintre cele care sunt pe cale să reuşească.

Mai rău decât atât este faptul că atacurile sunt din ce în ce mai sofisticate (sunt mai greu de detectat) şi mai distructive (băieţii răi ajung la chestiile bune). Gândeşte-te la detectorii de intruziune ca la nişte variante pentru internet ale sistemelor silenţioase de alarmă împotriva tâlharilor. Aceleaşi principii, la fel de vulnerabile, sunt înfrânte de tâlhari foarte pricepuţi sau, în acest caz, de hackeri. Cei mai experimentaţi hackeri ştiu de existenţa acestor detectori şi încearcă să pătrundă fără să fie descoperiţi. Dacă poţi face asta, ai şanse bune de a ajunge la informaţii militare clasificate. Poţi afla unde sunt trupele, ce fac, detalii despre funcţionarea armelor (astfel încât să te poţi apăra mai uşor de ele) şi, cel mai important, ai control asupra sistemelor de comunicaţii militare (care folosesc foarte mulţi sateliţi spaţiali).

Cu toate că cei mai mulţi dintre hackeri sunt doritori de senzaţii tari care încearcă apoi să se laude cu intruziunile lor şi cu „spargerea Pentagonului”, există şi unii destul de serioşi, care urmăresc un tipar şi au scopuri specifice şi periculoase. La sfârşitul anului 2001, Departamentul Apărării a raportat atacuri venite, se pare, dinspre al-Qaeda şi alte grupări islamice fundamentaliste. Cu toate că acele grupări nu dispun încă de cele mai avansate instrumente de hacking, există o mulţime de informaţii şi indicaţii pe internet despre „cum să devii hacker”, iar teroriştii atrag mulţi oameni educaţi pentru a se alătura acestor organizaţii. Primul virus informatic răspândit la scară largă a fost creat de programatori pakistanezi în anii ’80.

Nimeni nu publică date despre numărul de atacuri cyber-războinice făcute de armata americană. Evident, nu

vrei ca potenţialii inamici să ştie ce şi cum faci sau cât de des. Pentru că nicio altă naţiune nu are o prezenţă militară şi guvernamentală mai mare pe internet precum SUA, care au făcut investiţii mari în dezvoltarea tehnologiei şi a armelor pentru cyber-război. Spre deosebire de alte arme, pe cele folosite pe net nu le poţi identifica şi cu atât mai puţin descrie fără a le compromite eficacitatea. Aceasta continuă să provoace polemici în cadrul Departamentului Apărării atunci când unii lideri întreabă despre utilizarea formidabilelor arme cyber-războinice, iar cyber-războinicii rezistă, susţinând că ţinta nu este destul de importantă pentru a irosi realizările lor formidabile. Acest argument are sens. Odată ce unele dintre aceste tehnologii sunt folosite şi tehnicile sunt dezvăluite, nu mai sunt utile, sau cel puţin nu la fel de utile. Este aproape la fel ca în cazul grenadelor de mână, nu le poţi folosi decât o singură dată. Fără îndoială, nu există prea multe astfel de grenade în arsenalul cibernetic american. Şi atunci când sunt folosite, trebuie înlocuite cu costuri destul de mari. Mai mult, chiar şi armele existente devin rapid învechite pe măsură ce tehnologia internetului se schimbă.

Multe dintre atacurile asupra computerelor militare americane sunt depistate încă de la început, făcând astfel posibilă identificarea sursei lor. În multe cazuri, atacurile asupra PC-urilor erau lansate din centre de instruire operate de guverne, inclusiv cel al Rusiei, Chinei sau Irakului.

Un exemplu este un virus care a invadat PC-urile sediului central al marinei SUA pe 21 octombrie 1999. Atacul a distrus fişiere şi a oprit mai multe aparate. Virusul a exploatat vulnerabilităţile limbajului de scripting din Microsoft Word şi Microsoft Excel. Deşi nu au fost făcute publice detalii despre cum a fost lansat atacul, modul în care a fost dus la bun sfârşit a indicat faptul că a fost unul deliberat. Marina nu a raportat niciodată dacă a putut identifica sursa acestuia.

Mai îngrijorătoare sunt atacurile la scară largă lansate asupra reţelelor militare americane. Începând din martie 1998, au existat atacuri susţinute venite din Rusia. Guvernul rus îşi declină orice responsabilitate, cu toate că Statele Unite au protestat în mod formal împotriva ruşilor în 2000. Este foarte posibil ca atacul care a durat timp de trei ani să fi fost condus de bande criminale.

Furişarea în serverele militare şi lansarea unor programe zombie care pot fi uşor activate pentru a furniza hackerilor acces la date este o muncă profesionistă. Atacuri similare au avut loc asupra computerelor din universităţi şi organizaţii de cercetare.

PE URMELE URIAŞULUI

Spargerea anumitor „plase” îţi aduce mai multe puncte decât a altora. Cea mai mare miză o reprezintă armata SUA. Departamentul Apărării conduce aproximativ 10.000 de reţele diferite – majoritatea conectate la internet – şi foloseşte aproximativ două milioane de PC-uri. Aproape 2000 dintre „plasele” Pentagonului sunt critice, ele controlând funcţii esenţiale precum conducerea, armele nucleare, cercetarea şi informaţiile secrete.

În 1999, Pentagonul a depistat 22.000 de tentative de spargere a sistemelor. Cei mai mulţi dintre autori erau amatori, de multe ori „script kiddies” care utilizau instrumente facile, disponibile în număr mare pe web. În 2000, aceste tentative crescuseră cu aproximativ 10%. Cam trei la sută dintre ele au oprit unele pagini web şi reţele locale pentru o scurtă perioadă de timp. Cam unu la sută dintre aceste atacuri au reuşit să pătrundă pe un site, dar niciunul nu a putut ajunge la bazele de date clasificate sau n-a preluat controlul funcţiilor importante. Sau cel puţin nu au fost detectate astfel de cazuri. Îngrijorător pentru experţii de securitate de la Pentagon este numărul profesioniştilor care încearcă să pătrundă. Chiar şi în anii ’80, înainte ca internetul şi World Wide Web să devină foarte accesibile, agenţiile de informaţii secrete sovietice

angajau hackeri pentru a intra în reţelele Pentagonului. O parte dintre aceste încercări au reuşit. Un hacker profesionist vrea să intre, să obţină informaţiile şi să nu fie prins. Informaţiile clasificate furate în acest mod sunt mult mai valoroase decât acelea în care reuşeşti să intri, dar eşti descoperit. O parte dintre spargerile reuşite în ultima vreme au fost identificate ca venind din partea organizaţiilor militare din China şi Rusia. Ambele ţări neagă că ar fi încercat să spargă sistemele Pentagonului.

Armata a fost cea care a creat internetul, dar nu l-a folosit până când civilii nu au avut acces la el, la începutul anilor ’90, şi până nu a apărut World Wide Web. Nimeni nu se aştepta ca webul să aibă un aşa mare impact asupra modului în care comunică oamenii. Soldaţii, la fel ca şi civilii, au profitat de multe dintre oportunităţile oferite de web. Puşi faţă în faţă cu toată tevatura făcută pentru utilizarea webului în scop militar venită de la propriile trupe, generalii au cedat şi au început să folosească webul peste tot, chiar şi pe câmpul de luptă. Cu toate acestea, li s-a amintit tuturor cât de uşor este să pătrunzi pe site-urile web ale altora şi în serverele pe care acestea le folosesc. Hackingul nu era singura problemă.

La începutul anului 2000, Pentagonul a privit cu mai multă atenţie 800 de site-uri web militare mai importante. Au descoperit 1.300 de situaţii în care informaţii exacte sau chiar clasificate deveneau disponibile. La scurt timp după aceea, majoritatea site-urilor web militare au fost închise pentru „reorganizare”. Atunci când au reapărut, existau mult mai multe restricţii cu privire la cine avea acces la date şi în ce măsură. Fie aveai nevoie de un cont militar (mii), fie de o parolă pentru a ajunge la chestiunile importante. Mai puţin vizibile erau schimbările dese pentru a încerca să ţină hackerii la distanţă.

Cea mai bună apărare împotriva hackerilor sunt administratorii de sistem bine pregătiţi, care actualizează software-ul şi îl păstrează în siguranţă. Majoritatea

hackerilor, mai ales cei profesionişti, reuşesc ceea ce-şi propun din cauza software-urilor prost instalate sau neactualizate cu ultimele update-uri şi protecţii. Cererea de administratori de sistem buni i-a făcut imediat pe tinerii soldaţi care aveau aceste aptitudini să fie gata pentru angajare pe piaţa de muncă civilă. De fapt, armata a avut ceva de furcă încercând să îi facă să se înroleze din nou. Fiind atât de greu să păstreze suficienţi administratori de sistem, serviciile foloseau adesea civili care declarau că ştiu „câte ceva despre PC-uri”.

Criza de administratori de sistem a fost abordată printr-un suport pentru site-urile web militare mai bine centralizat. Apoi, la sfârşitul anilor ’90, armata a început să folosească propriile echipe de hackeri pentru a-şi ataca periodic site-urile personale şi reţelele, astfel încât să vadă cât de sigure sunt. Site-urile vulnerabile au atras mai multă atenţie. Nu era o soluţie perfectă, dar era mai bine decât anarhia de dinainte.

În acelaşi timp, Pentagonul a trecut în ofensivă. Site-urilor cu probleme li se acorda cea mai mare atenţie, fapt ce nu se făcea înainte. Pentru a micşora numărul atacurilor reuşite efectuate de către amatori, pe hard diskurile serverelor erau puse fişiere false, etichetate ca secrete de maximă importanţă. Aceste momeli ademeneau impostorii să stea suficient de mult timp pe site-uri, astfel încât să fie prinşi sau cel puţin identificaţi (de obicei erau chinezi sau ruşi). Câteva urmăriri penale aveau să descurajeze mulţi hackeri de ocazie. Cu profesioniştii este o altă problemă. Aceştia sunt precauţi şi talentaţi. Ei pătrund pe un site, caută să vadă dacă sunt capcane şi analizează cât de bine este pusă la punct securitatea. Apoi vor reveni şi vor provoca pagube reale, ştiind cum să nu declanşeze alarmele. Aşa cum am mai spus, nu numai fişierele furate provoacă îngrijorare, ci şi implantarea acelor programe care pot fi lansate mai târziu pentru a şterge reţeaua şi fişierele sau care pot trimite date operaţionale inamicului.

Acestea din urmă sunt în mod special înfricoşătoare, întrucât înseamnă că inamicul va avea informaţii despre ce anume face acel calculator, mai precis planurile tale în vederea războiului.

Nimeni nu a lansat încă un atac major pe net, dar există posibilitatea. SUA, care deţin mai multe PC-uri şi reţele decât oricare altă naţiune, par să fie mai vulnerabile la astfel de ofensive. Dar şi cea mai mare parte din munca depusă pentru securitatea reţelelor este realizată tot în SUA. Nimeni nu ştie cât de probabil este un război web, dar nimeni nu crede că este imposibil. Cineva va deveni, în cele din urmă, victimă a unui atac „Pearl Harbor" lansat de hackeri. Până atunci, oricine este eligibil pentru această onoare îndoielnică.

INTERNETUL MERGE LA RĂZBOI

Nu a existat nicio magie în faptul că internetul a fost adoptat rapid pentru utilizarea militară. Presiunea şi insistenţa veneau din partea cadrelor inferioare. Soldaţii au cumpărat PC-uri cu bani proprii înainte ca astfel de achiziţii să fie făcute oficial. Trupele au văzut imediat ce economie a efortului aduceau PC-urile şi e-mailul. Apoi, când Departamentul Apărării a aprobat, în cele din urmă, ca internetul să fie „comercializat", la începutul anilor '90, trupele au fost încântate. Dar atâta vreme cât internetul era legat de liniile telefonice, o mare parte din utilizarea sa se limita la bazele militare şi la soldaţii care îşi foloseau PC-urile acasă pentru a păstra legătura unii cu alţii. Chiar înainte ca internetul să devină disponibil pentru marele public, soldaţii foloseau ARPANET (procesorul DOD al internetului) şi reţelele comerciale pentru a discuta probleme militare, a planifica operaţiuni şi în general pentru a opera mai rapid şi mai eficient. De obicei, generalii erau ultimii care aflau de ce instrument puternic dispuneau. Într-adevăr, o mare parte din generalii din anii '90 au încercat pentru prima dată internetul pe când erau

studenţi sau subofiţeri. Acest lucru a jucat un rol major în conexiunea rapidă la internet şi la e-mail dintre ei şi organizaţiile militare din Statele Unite. Generalii au observat că această metodă este mai rapidă şi mai eficientă decât cele tradiţionale de comunicare (telefonul, documentele scrise).

După Războiul din Golf, cuvintele care făceau vâlvă erau „operaţiuni centrate pe net”. Ofiţerii au început să caute trupe tinere cu cunoştinţe despre internet. Ofiţerii superiori şi-au văzut propriii copii, la fel ca şi pe subofiţerii care lucrau pentru ei, entuziasmaţi de internet, în plus, mulţi ofiţeri militari sunt pasionaţi de gadgeturi şi sunt fani science fiction. Internetul a atins o coardă sensibilă, ceea ce a condus la aplicarea lui mai rapidă în sistem. Odată acceptată oficial această tehnologie, au început să se pună lucrurile la punct. De exemplu, echipamentul de sateliţi a fost reglat pentru a face faţă datelor de pe internet. Armata a folosit o variantă sigură (criptată) a datelor de pe internet pentru a putea trimite în siguranţă materiale de la un browser la altul. Marina şi-a actualizat comunicaţiile, astfel încât fiecare marinar să poată folosi e-mailul ori de câte ori doreşte. Nu numai că astfel s-a uşurat munca tuturor şi s-a făcut mai rapid, dar a fost îmbunătăţit şi moralul celor care erau obligaţi să stea mai multe luni pe mare. Comandanţii de pe câmpurile de luptă ale armatei foloseau browserele web pentru a înlocui telefoanele din teritoriu şi hărţile învelite în plastic (şi creioanele), care fuseseră instrumentele lor cheie timp de aproape un secol.

Jocurile online şi comunicaţiile interactive vocale şi grafice au furnizat trupelor concepte şi tehnologie de lucru pentru a crea tehnici de luptă care măreau viteza operaţiunilor, astfel încât un oponent care nu era centrat pe net să nu poată ţine pasul. Întotdeauna este nevoie de viteză pe câmpul de luptă, iar instrumentele internetului furnizează mai multă viteză decât îşi poate închipui cineva.

Cu toate acestea, potenţialii oponenţi au şi ei acces la instrumentele de pe internet, aşa că nu era un lux pentru armată să adopte această tehnologie. Oricine ar implementa internetul în luptă va avea un avantaj, unul care poate face diferenţa dintre viaţă şi moarte. La începutul erei Silicon Valley dot.com, puţini oameni s-au gândit la browsere ca la arme letale, dar asta sunt. Cel care ajunge primul pe câmpul de luptă cu cea mai avansată tehnologie a internetului va supravieţui şi va câştiga.

AMENINŢAREA DINSPRE EST

Războiul Rece trebuia să se fi terminat în 1991, dar, pe internet, el continuă. Gândeşte-te la lupta dintre bandele criminale ruseşti şi experţii software ai Războiului Rece din 2000. Bandele au pătruns în trei duzini de site-uri de comerţ electronic foarte bine păzite şi de instituţii financiare şi au furat date de la peste un milion de conturi de cărţi de credit. Aceste bande sunt considerate a fi dintre cele mai periculoase din spaţiul cibernetic. Deşi guvernul rus a început să lovească în aceste grupuri din 2001, ele sunt atât de bogate, de bine conectate şi de violente, încât orice înlăturare a lor va fi dificilă. Celălalt duşman al Războiului Rece, China, nu este deloc interesat să îşi ţină în frâu hackerii. În aprilie 2001, hackerii chinezi s-au mobilizat pentru distrugerea site-urile web americane în semn de protest pentru patrulele aviatice americane care au doborât un luptător de-al lor în acea lună. Chinezii nu s-au descurcat prea bine, au afectat cel mult 300 de site-uri, în vreme ce hackerii americani au distrus, din răzbunare, peste 900 de site-uri chinezeşti. Neresemnaţi, hackerii chinezi se pare că au lansat viermele Code Red, care a doborât peste 300.000 de site-uri (majoritatea americane). Code Red a fost identificat ca venind de la o universitate din China.

Această ţară susţine deschis că cyber-războiul este o

zonă în care poate dobândi capacităţi la nivel mondial şi poate egala America. Din cauza numărului tot mai mare de atacuri ce au ca ţintă SUA a căror sursă a fost identificată ca venind din China, inclusiv de la serverele guvernului, nu se poate trage decât o concluzie: chinezii au intenţii serioase.

JUDECATA DE APOI PE INTERNET

În 2000, doi studenţi ruşi din Kaluga au fost arestaţi, judecaţi şi condamnaţi pentru o înşelătorie pe internet. Cei doi au încercat să se dea drept ofiţeri răspunzători de lansarea rachetelor nucleare ruseşti. Voiau să atace cu arme nucleare Europa de Vest. Ambii au fost condamnaţi la un an de muncă silnică. Implicaţiile acestei acţiuni au devenit o problemă – pentru toată lumea. Cel puţin teoretic, este posibil să spargi site-uri pentru a face ceva atât de periculos.

GHERILELE ELECTRONICE DIN CHINA

Pentru că noile tehnologii tind să aducă schimbări pe care guvernele nu le pot controla, China a intrat agitată în secolul XXI. Timp de secole, ţara a rezolvat astfel de probleme subminând schimbarea. Nouă ne poate părea ciudat, dar a funcţionat în China de multe ori, iar liderii lor nu văd nimic rău în această abordare. China este încă un stat poliţienesc, iar guvernul se teme de o mişcare populară care ar putea înlătura controlul partidului comunist. Până acum, guvernul a insistat să controleze mass-media şi comunicaţiile.

Cu toate acestea, cea mai mare problemă a guvernului este corupţia, nu revoluţionarii. Corupţia în creştere, mai ales printre membrii partidului comunist, aflat la putere, face din comunicaţiile nesistematizate dintre cetăţeni o sursă de schimbare politică nedorită pentru guvern. Dezvoltarea mass-mediei secolului XX a schimbat modul în care operează politica în China. Mass-

media electronică şi mai ales radioul au făcut ca o populaţie în mare parte analfabetă să fie mult mai conştientă de lumea de dincolo de satul lor. Răspândirea televiziunii din ultimii 20 de ani nu a făcut decât să amplifice acest lucru. Apoi au venit pagerele, telefoanele mobile şi internetul în anii ’80 şi 90. Pentru un guvern totalitar, aceasta a fost o schimbare înspăimântătoare. Mass-media controlată, precum radioul şi televiziunea, făcea ca statul poliţienesc să fie condus mai uşor. Puteai controla mesajele sau nu lăsai oamenii să ştie, de exemplu, cât de mult rău face partidul comunist. Chiar şi telefoanele pot fi controlate prin limitarea numărului celor care le deţin şi explicând tuturor ce este o ramificaţie telefonică. Pagerele şi celularele erau mobile şi de aceea cu atât mai periculoase. Internetul era şi mai rău, întrucât permitea accesul la lumea exterioară. Cel mai rău dintre toate era că nu exista un istoric despre cum trebuie manevrate aceste tehnologii. Comuniştii conduc cam în acelaşi mod în care o făceau împăraţii cu mii de ani în urmă.

Spre sfârşitul secolului XX, chinezii au restricţionat internetul, faxul şi telefoanele mobile. Deşi toate aceste eforturi nu sunt în totalitate eficiente, disidenţii chinezi sau criminalii ştiu că întotdeauna există posibilitatea să fie ascultaţi de o altă ţară. Cyber-poliţia chineză a încercat să codifice exprimarea pe net şi a creat o generaţie de gherile electronice. E-mailul, faxul şi telefoanele mobile folosesc la rândul lor cuvinte codificate. Website-uri conţinând informaţii secrete sunt localizate în afara Chinei. Când cyber-poliţia află despre ele şi le blochează, site-ul se mută, iar mesaje codificate explică unde pot fi găsite ulterior. Totuşi, utilizatorii de internet din China trebuie să aibă grijă. Este ilegală folosirea criptării. Dacă eşti prins, vei avea o întrevedere cu poliţia secretă şi rişti să petreci mult timp în închisoare. În China, sistemele de telefonie mobilă sunt setate astfel încât să poată fi găsită rapid locaţia utilizatorilor. Dacă faci parte dintre suspecţi,

trebuie să fii precaut atunci când îţi foloseşti mobilul. Poate fi scump să cumperi în permanenţă altele şi de asemenea poate alerta poliţia. Utilizarea faxului poate fi depistată cu ajutorul liniei telefonice.

Există gadgeturi wireless care le dau bătăi de cap celor de la poliţia cibernetică din China: pagerele. Ele au fost prima formă de comunicare wireless introdusă în China, foarte populare, întrucât erau mult mai ieftine. În anul 2000 existau aproximativ 1.500 de sisteme de pager, cu 52.000 de staţii de bază (antene) şi peste o sută de milioane de utilizatori (comparativ cu 60 de milioane de utilizatori de mobile, 12 milioane de utilizatori de internet şi 130 de milioane de utilizatori ai telefoanelor obişnuite din această ţară). Supravegherea pagerelor este dificilă deoarece există atât de multe companii diferite care furnizează acest serviciu şi atât de mult coduri. Era, practic, imposibil să captezi toate sau aproape toate mesajele. Chiar dacă reuşeau, sortarea mesajelor care spuneau „ia nişte mazăre dulce în drum spre casă" de cele care transmiteau „demonstraţia va avea loc mâine la 13" ar fi depăşit tehnologia actuală. Astfel chinezii folosesc liberi pagerele pentru a comunica fără ca Fratele cel Mare să tragă cu ochiul. Cu ajutorul pagerelor (şi majoritatea mobilelor care permit şi ele mesajele text), grupul religios persecutat Falungong a putut să-şi menţină organizaţia şi a continuat să facă demonstraţii. Dezavantajul este că organizaţiile criminale folosesc şi ele pagerele, complicând munca poliţiei.

Oricât de ieftine şi de utile ar fi pagerele, utilizarea lor se află în declin întrucât serviciile de telefonie mobilă se răspândesc în China. La sfârşitul anului 2001 existau 135 de milioane de utilizatori de mobile şi numai 50 de milioane de utilizatori de pagere. Deşi este mai scump decât mobilele şi pagerele, internetul se afla şi el pe linie ascendentă, ajungând la 22 de milioane de utilizatori (de la mai puţin de două milioane în 1997). Spre disperarea

poliţiştilor cibernetici, vechii utilizatori de pagere aduc tuturor tehnologiilor cibernetice din China obiceiul de a folosi coduri şi limbaje argotice. Deşi tot mai mulţi chinezi aveau telefoane mobile, ei preferau să scrie mesaje scurte. Cu atât de mulţi oameni care folosesc coduri pentru uz practic (economic), este dificil pentru poliţişti să îşi dea seama când acel uz este nevinovat şi când nu.

Totuşi, poliţia are un avantaj unic. Poliţiştii cibernetici din China sunt cel mai bine pregătiţi şi mai experimentaţi din lume atunci când vine vorba despre dejucarea sau monitorizarea comunicaţiilor pe internet sau wireless. Acest lucru are implicaţii dincolo de nevoia de a conduce un stat poliţienesc într-o epocă a internetului. Îţi oferă un pas în afara limitelor tale. Să lucrezi ca hacker pentru poliţie este o slujbă prestigioasă în China. Guvernul s-a jucat cu naţionalismul în ultimii zece ani şi acest lucru a fost bine primit de către cei tineri. Propaganda pune accent pe recuperarea remarcabilă a Chinei după un secol de calamităţi şi pe nevoia de a primi respect din partea celorlalte naţiuni. Este acelaşi tip de naţionalism care a dus la declanşarea Primului şi a celui de-al Doilea Război Mondial. Politicienii comunişti care conduc China se joacă cu focul, dar funcţionează. Aşa că hackerii se înscriu bucuroşi pentru a-şi servi patria. În mod remarcabil, numai câţiva au fost „poluaţi” de ideile din Vest. Democraţia este un concept străin Chinei, iar cei care o văd ca pe o necesitate sunt numai câţiva. Nu vor decât să fie lăsaţi în pace de guvern ca să se poată îmbogăţi.

Cu toate acestea, China are o problemă cu hackerii ei. Spre deosebire de India, cealaltă putere în materie de software, China predă studenţilor programarea în chineză. Studenţii din India învaţă aceste lucruri în engleză, ceea ce le conferă un mare avantaj. Mai mult, studenţii indieni tind să fie mai familiarizaţi cu produsele Microsoft care sunt cel mai des folosite. În China, standardul este Unix, cu alte cuvinte, Linux. De fapt, universităţile chineze nu permit

decât folosirea Linuxului. Astfel, cyber-războinicii chinezi trebuie să înveţe mai târziu cum să folosească software-ul Microsoft (cel mai vulnerabil din lume şi cel mai des folosit de organizaţiile guvernamentale din SUA).

Deşi chinezii sunt cei mai buni de pe planetă în folosirea pagerelor, mobilelor şi a internetului, ei ştiu că acest lucru s-ar putea să nu fie suficient. Această capacitate probabil se va dovedi mai utilă ca armă împotriva duşmanilor străini. Taiwan şi SUA au primit deja o mostră neplăcută cu ceea ce pot face hackerii guvernului chinez. Între timp, hackerii din China se mişcă în moduri pe care nimeni nu le poate prevedea. Dacă această ţară scapă de sub control, poţi să fii sigur că pagerele şi telefoanele mobile sunt cele de la care a pornit totul

CYBER-RĂZBOINICII FLĂMÂNZI AI IRAKULUI

Nu toate exemplele de cyber-război implică abilităţi tehnologice, dar necesită un grad de imoralitate. Iată un exemplu care s-a desfăşurat chiar sub ochii tăi. Irakul continua să protesteze că embargoul Naţiunilor Unite omoară civili irakieni. Acest embargo exista de la sfârşitul Războiului din Golf în 1991 şi nu avea să se sfârşească decât atunci când Irakul ar fi permis inspectorilor de arme să certifice faptul că nu produce arme nucleare, chimice sau biologice. Cum Irakul a refuzat să dea drumul inspectorilor, embargoul a continuat. În mod particular, acest embargo împiedica Irakul să cumpere anumite tipuri de camioane de mare tonaj, computere, echipament chimic sau industrial. Naţiunile Unite susţineau că acest tip de echipament are dublă utilizare şi că putea fi folosit de armată pentru producerea armelor chimice. Irakienii erau dornici să poată avea un impact cyber-războinic serios. Această ţară are mulţi ingineri angajaţi cu sume mici, mulţi dintre ei sunt talentaţi şi destul de patrioţi; nu au nevoie decât de echipament. De fapt, SUA sunt cele care se opun îmbarcării acestor elemente spre Irak. Principalul

motiv este acela că, atunci când a permis o astfel de îmbarcare în anii ’80, a fost acuzată la ceva vreme de „înarmarea Irakului”. Acesta a devenit un mit popular de stânga. O carte tipică de acest fel a fost *Arming Iraq* (de Mark Phythian şi Nikos Passas): „Cum construiesc SUA şi Marea Britanie în secret maşina de război a lui Saddam”. Editura Northeastern University a publicat această carte, ce are ca subiect traficul de arme din timpul Războiului dintre Iran şi Irak şi despre cum a distrus Irakul programele de ajutor pentru a cumpăra arme şi cum a exploatat echipamentul cu dublă utilizare. PBS a realizat o emisiune în septembrie 1990, aruncând vina asupra Vestului pentru înarmarea Irakului, folosind aceleaşi dovezi. Cumva, nimeni nu a venit cu dovezi concrete (cu excepţia francezilor, dar asta nu era secret) că Irakul deţinea arme americane. Toată această paranoia a fost transformată în „Irakgate”, o conspiraţie americană de amploare pentru formarea forţelor armate irakiene. Singurele „arme” identificate au fost echipamentele nonmilitare (echipamente medicale, camioane, substanţe chimice industriale etc.) care au fost folosite în scop militar, mai ales la fabricarea armelor chimice. Atunci când SUA au încercat să împiedice folosirea acestor echipamente cu dublă utilizare, aceiaşi oameni care au inventat „Irakgate” au acuzat America de abuz asupra civililor. Cine zice că nu poţi avea totul? Dar internetul facilitează întoarcerea pe toate părţile a unei poveşti şi mobilizează oamenii de pe întreg globul. Deşi Irakul nu a putut să construiască o forţă cyber-războinică, este evident că a împânzit internetul cu minciuni. Toate acestea au atras susţinerea la nivel mondial a unui stat poliţienesc criminal. Totuşi, este evident că guvernul irakian este responsabil pentru creşterea ratei decesului din 1991 încoace şi acest lucru poate fi subliniat de mult mai înaltele standarde de viaţă din nordul Irakului (cu o rată mai mică a deceselor), unde Naţiunile Unite au înlăturat

guvernul irakian de la începutul anilor ’90 (pentru a-l împiedica să înceapă un alt masacru asupra populaţiei kurde). Nu ai nevoie de multe computere pentru a purta o campanie victorioasă de cyber-război.

Între timp, este imposibil să împiedici intrarea PC-urilor în Irak, întrucât sunt prea mulţi pungaşi care operează dincolo de graniţele ţării. Dar blocarea marilor ambarcaţiuni cu aceste echipamente, mai ales serverele şi ruterele mai scumpe cu care ar vrea să se joace hackerii în formare ai lui Saddam, limitează gradul de letalitate al cyber-războinicilor irakieni. Iar în acest domeniu chiar şi cel mai mic lucru ajută.

LEGĂTURILE SLABE SCUFUNDĂ NAVE

Gândeşte-te că majoritatea trupelor au acum conturi de e-mail. Deşi este puţin probabil ca cei de pe teren să le folosească prea mult, cei care stau într-un singur loc o fac. Pentru marinari, care nu pierd niciodată accesul la e-mail cât timp sunt la bordul navelor, marina a stabilit reguli clare cu privire la ce poate fi transmis pe această cale. De asemenea, marina monitorizează şi scanează emailurile trimise pentru cuvintele-cheie. Totuşi, o remarcă inocentă (care nu conţine cuvinte pe care să le surprindă scanerul) despre amplasamentul navei poate ajunge acasă. Înainte să îţi dai seama, tipii răi ştiu lucruri pe care nu ar trebui să le ştie. Cyber-agenţii inamici nici nu trebuie să se bazeze pe e-mail. Există sute de buletine informative pentru familiile militarilor. Aici, oamenii din armată şi membrii familiilor lor discută probleme de interes comun. Un agent inamic îi poate descoperi, supraveghea şi culege tot felul de informaţii utile. Poate că nu este genul de lucruri care să atragă un reporter, dar cu toate acestea pot ieşi la suprafaţă informaţii cu potenţial letal. Dacă cei care folosesc aceste buletine nu sunt atenţi, agenţii inamici pot afla informaţii despre moralul trupelor, locaţia unităţilor şi activitatea lor. Este o problemă veche. În timpul celui de-al

Doilea Război Mondial, existau postere pe zidurile magazinelor şi saloanelor cu sloganul „Gurile slobode scufundă navele”. În 60 de ani, foarte puţine lucruri s-au schimbat, numai că acum oamenii îşi petrec timpul pe internet, unde cineva din orice parte a lumii îi poate asculta.

CONSILIUL NAŢIONAL DE ASIGURARE A INFRASTRUCTURII (CNAI)

Una dintre ultimele activităţi ale lui Bill Clinton în calitate de preşedinte a fost să înfiinţeze o altă organizaţie de consiliere pentru securitate: Consiliul Naţional de Asigurare a Infrastructurii (CNAI). Acest lucru îmi aminteşte de vechiul banc despre cum rezolvă un politician o problemă pe care nu vrea să o rezolve: înfiinţarea „unui grup de primă clasă” (format numai din oameni de primă mână) pentru a studia problema la sânge sau cel puţin pentru a o pune într-o gaură neagră, astfel încât mass-media să îşi piardă interesul. Acest grup concurează acum cu echipe precum CNAI, care sună pompos, face puţine şi este în general ignorat. Atenţia tot mai mare pe care o acordă mass-media securităţii comunicaţiilor şi internetului a dus la înfiinţarea a sute de grupuri, comitete şi studii. De exemplu, acestea sunt numai câteva dintre organizaţiile similare (care duc peste ocean politica naţională a internetului) la care s-a alăturat CNAI: Computer System Security and Privacy Advisory Board (Departamentul Comercial al acestei instituţii), Centrul Naţional de Protecţie a Infrastructurii, Oficiul de Urgenţă pentru Asigurarea Infrastructurii, Consiliul Naţional de Ştiinţă şi Tehnologie, Grupul de Coordonare a Incidentelor Cibernetice (CIA, NSE, CIAO, FBI şi altele), Agenţia Naţională de Securitate, Departamentul Apărării, Consiliul Naţional de Securitate, Consiliul Federal de Relaţionare, Oficiul de Management şi Buget, Comitetul Federal de Supraveghere a Infrastructurii Publice, Consiliul Extern de

Criptare al Preşedintelui, Consiliul de Dezvoltare a Tehnologiei Informaţionale, Comitetul Prezidenţial de Consiliere pentru Tehnologia Informaţională.

Cei care sunt consiliaţi în acest sens consideră toate aceste eforturi inutile, ba chiar uneori contraproductive. Nimeni din grupurile de consiliere nu vorbeşte aceeaşi limbă sau cu suficientă autoritate pentru a atrage atenţia celorlalţi. Astfel ai parte de un murmur confuz pe care nimeni nu îl înţelege şi căruia nimeni nu îi acordă atenţie. Acum ştii.

HACKERI PATRIOŢI

Poate că atacurile din 11 septembrie 2001 nu au adus represalii imediate în ceea ce priveşte acţiunile militare, dar au fost o mulţime de operaţiuni cyber-războinice care au avut loc repede. Site-urile web asociate cu radicalismul islamic au fost atacate de necunoscuţi (se bănuieşte că erau antiterorişti americani), de obicei având ca rezultat doar distrugerea acelor pagini. Prima pagină era înlocuită, de cele mai multe ori, cu un mesaj sau o imagine antiteroristă sau cu vreun simbol patriotic. Poate că cel mai distrugător atac a fost unul neobişnuit. În Germania, un hacker, ce se autointitula „Anonyme Feigling”, a spart un server ce găzduia un *listserv* (un grup de discuţii pe email) ce susţinea războiul sfânt islamic şi terorismul. A luat 500 de nume de pe lista de e-mailuri şi le-a publicat pe internet. De asemenea, a alertat poliţia şi a dezvăluit adevărata sa identitate. Poliţia nu a luat nicio măsură împotriva lui. O persoană din cele aflate pe listă era deja căutată de FBI. Acest tip de atac este neobişnuit din mai multe puncte de vedere, întrucât multe *listservere* consideră că este esenţial să ţină secretă identitatea participanţilor pentru a încuraja discuţiile libere.

Dar există şi *listservere* pro-teroriste (sau alte acţiuni ilegale). Cele mai multe *listservere* islamice tind să fie pro-teroriste şi de asemenea există multe care discută despre

politica de stânga. Multe dintre acestea au dispărut ori şi-au schimbat subiectele de discuţie după 11 septembrie 2001. Site-urile pro-talibane sau cele similare s-au aflat sub atac constant începând cu 11 septembrie 2001. Conţinutul obişnuit a fost înlocuit de nenumărate ori cu postere pentru găsirea lui Osama bin Laden sau cu altele de acest gen. De asemenea, au fost negate atacurile de serviciu. O parte dintre aceste site-uri au fost închise, iar altele au fost înlăturate de pe net de către furnizori. Alţi hackeri au mers mai departe, chiar până la spargerea site-ului unei bănci sudaneze unde au fost găsite date despre conturile bancare ale lui bin Laden, informaţii care au fost transmise FBI. Această acţiune de hacking a fost făcută publică, dar existau suspiciuni şi cu privire la altele asemănătoare. Nu au existat rapoarte despre judecarea acestor hackeri, cu toate că aceştia recunosc că ce au făcut a fost ilegal.

Acest tip de război a continuat, deşi nu s-a bucurat de prea multă publicitate. Se pare că au existat mai multe spargeri oficiale ale site-urilor pro-teroriste, care căutau nume, mesaje tip avizier şi tot felul de informaţii utile. Legea, în special cea internaţională, este încă destul de vagă în privinţa spargerilor site-urilor de către guvern sau a altor forme de atac pe internet. Dar cum aproape fiecare naţiune din lume s-a înscris pentru războiul împotriva terorismului, avocaţii şi curţile de judecată au păstrat tăcerea cu privire la aceste probleme.

Hackerii s-au alăturat, voluntar, de fiecare dată când ţara lor era implicată într-un conflict armat sau doar diplomatic. Ruşi, chinezi, pakistanezi, arabi, israelieni, americani şi alte naţionalităţi de împătimiţi ai internetului s-au alăturat luptei pe cont propriu. Un exemplu recent (la începutul anului 2002) a avut loc în Tomsk, Siberia, Rusia. FSB-ul (FBI-ul rusesc[2]) a descoperit în oraş şapte hackeri

2 FSB (ФСБ - Федера́льная слу́жба безопа́сности Росси́йской Федера́ции; transliterat *Federal'naia slujba bezopasnosti Rossiiskoi*

care porniseră propriul război împotriva rebelilor ceceni în ultimii trei ani. Unul dintre cei şapte era din Groznîi (capitala republicii ruseşti Cecenia). Asemenea multor ruşi care locuiau aici, acesta plecase pentru a evita campania sângeroasă a etnicilor pentru a-i scoate pe ceceni afară. Astfel inspirat, el a cooptat şase utilizatori ruşi de computere pentru a porni propriul război împotriva cecenilor. Cei şapte, toţi studenţi, au atacat orice site pro-cecen peste care au dat. Unul dintre ele, „Kavkaz”, a fost forţat să schimbe ISP-urile de trei ori şi tot se mai afla sub atac. Studenţii recrutează tot mai mulţi hackeri ruşi pentru aceste acţiuni. FSB-ul i-a lăsat pe mulţi în pace.

AFGANISTAN

Războiul din Afganistan a izbucnit la începutul lui octombrie 2001 cu atacuri aeriene asupra ţintelor militare talibane. Cam în aceeaşi perioadă, trupele americane şi engleze au atacat la sol. De asemenea, acesta a fost primul război în care internetul (şi alte reţele) a jucat un rol important. Cu zece ani mai devreme, în 1991, internetul era încă o operaţiune minoră, una dintre multele reţele de computer. World Wide Web nu fusese încă inventat. Dar în 2001, toată lumea era pe internet sau ştia de existenţa lui. În zece ani, conceptul de a face parte dintr-o reţea de comunicaţii electronice era considerat ca fiind ceva firesc. Acest lucru a fost pus în practică pe terenul din

Afganistan, întrucât trupele forţelor speciale americane au aterizat şi au trecut la treabă. Au pus imediat la punct o reţea unică folosind bombardierele americane, sateliţi şi avioane de recunoaştere, precum şi diverşi lideri militari şi politici americani din afara Afganistanului. Scopul acestei reţele era de a direcţiona rapid o tonă de explozibil înspre ţintele inamice.

Arma cea mai impresionantă folosită a fost JDAM

Federației) este serviciul secret al Federației Ruse și este succesorul KGB-ului. Sediul central se află în Moscova.

(Joint Direct Attack Munition), o bombă de o tonă ghidată de semnale primite de la sateliţi (sistemul GPS) spre o ţintă selectată de cineva de la sol care folosea un aparat de identificare cu laser şi un radio pentru a transmite locaţia unei aeronave de deasupra. Cei de la sol primeau de asemenea informaţii de la avioane de recunoaştere şi sateliţi, care le ofereau, la propriu, o imagine de dincolo de dealul din faţa lor. Comunicaţiile prin satelit trimiteau aceste fotografii (şi imagini în mişcare), dar şi conversaţiile soldaţilor de la sol înapoi la Pentagon şi Casa Albă. Toate acestea aveau loc în timp real.

Aceea era o reţea destul de complexă (echipa de la sol care folosea radioul, GPS-ul şi laserul pentru a comunica cu bombardierul de deasupra, care la rândul lui folosea GPS-ul, radioul şi chiar bomba, care la rândul ei folosea GPS-ul pentru a găsi ţinta desemnată de echipa de la sol). Semnalele radio şi GPS pot fi distruse. Dar în Afganistan nu s-a întâmplat acest lucru pentru că inamicul nu putea face faţă vitezei unei astfel de tehnologii. Nu numai că semnalele slabe de GPS pot fi interceptate, dar pot fi şi modificate. Acest lucru putea fi făcut pentru a direcţiona JDAM-ul către trupe proprii. Doar pentru că tehnologia mai puţin avansată a talibanilor nu a „spart reţeaua JDAM” nu înseamnă că nu ar putea să o facă altcineva, sau că nu va încerca cel puţin.

Trupele americane ştiu că le-a fost mai uşor în Afganistan pentru că nimeni nu a încercat să interfereze cu reţeaua lor de pe câmpul de luptă. Totuşi, data viitoare, lucrurile vor deveni probabil mai interesante dacă duşmanul va încerca acest lucru, iar defensiva secretă a reţelei este supusă testelor.

SITE-UL AL-QAEDA, ATACAT ÎNAINTE DE RĂZBOI

Chiar şi înainte de 11 septembrie 2001 a existat o campanie cyber-războinică împotriva reţelei teroriste al-

Qaeda. Se raportează că au foii sparte conturi bancare de către agenţiile secrete americane, iar fondurile au fost şterse sau transferate. Chiar dacă în majoritatea cazurilor spargerea a fost făcută doar pentru a aduna informaţii despre locurile sau resursele grupării, atunci când se ivea posibilitatea unui atac, de e ele mai multe ori se profita de ocazie.

Comunicaţiile prin telefoane mobile şi sateliţi au fost de asemeni interceptate.

Existau aproximativ 200 de site-uri care susţineau al-Qaeda sau alte grupări teroriste islamice, care erau şi ele vizate, sau sparte pentru a obţine acces la computere ce conţineau mai multe date. În acest fel, au fost obţinute informaţii despre terorişti, susţinătorii lor şi contribuitori. În ciuda acestui efort, nu s-a depistat nimic despre planificarea atacurilor din 11 septembrie.

Teroriştii au prins de veste despre atacurile asupra comunicaţiilor lor pe internet la mijlocul anilor ’90 şi au răspuns prin intensificarea apărării cibernetice şi prin folosirea intensă a criptării, al-Qaeda folosise întotdeauna cuvinte codate şi, începând cu mijlocul anilor ’90, a început să folosească criptarea. Mai târziu s-a descoperit că pentru operaţiunile-cheie (precum atacurile din 11 septembrie) mesajele erau trimise numai prin curier şi niciodată prin telefon sau internet. Dar FBI şi

CIA nu ştiau de acest act adiţional de apărare în al-Qaeda şi credeau că deţin controlul comunicaţiilor teroriştilor.

Cea mai mare parte a acestei monitorizări era făcută din umbră, întrucât gradul de legalitate al acesteia este încă destul de discutabil. De exemplu ai nevoie de o hotărâre judecătorească pentru a supraveghea conversaţiile telefonice în America, dar nu şi peste ocean. Practic, guvernul poate monitoriza traficul pe internet fără această hotărâre, dar se poate aştepta la chemări în judecată de la grupuri de civili atunci când aceste

supravegheri sunt făcute publice.

Convenţiile de la Geneva, care de mai bine de un secol au stabilit unele repere legale în privinţa războiului, nu au fost încă modificate pentru a acoperi şi cyber-războiul. Legea civilă pentru interceptarea internetului este în proces de a fi schimbată, dar aceasta va dura fără îndoială mai mulţi ani.

STRIVIT DE INTERNET

Deşi peste 20.000 de terorişti islamici s-au grupat în Afganistan în timpul războiului împotriva terorismului (şi în alte ţări unde existau tabere de formare), cea mai mare parte dintre ei erau trataţi ca infanterie, folosiţi ca trupe la sol pentru a se lupta cu Alianţa Nordică pentru talibani, iar dacă supravieţuiau, erau trimişi acasă, să facă ce pot pentru a obţine victoria islamului. Cei mai mulţi dintre ei s-au limitat la o conversaţie antrenantă la o cafenea locală sau la moschee.

Cum ştim toate acestea? Se pare că, printre materiile predate celor din şcolile al-Qaeda, securitatea operaţională nu era printre cele preferate. OPSEC (securitatea operaţională) face ceea ce este nevoie pentru a împiedica duşmanul să afle ce pui la cale. Adepţii al-Qaeda au înţeles nevoia de OPSEC, dar mulţi nu au înţeles măsura în care aceasta trebuia pusă în practică pentru a rămâne nedetectată. Cea mai mare slăbiciune a al-Qaeda era folosirea neprecaută a telefoanelor (mai ales a celor mobile) şi a e-mailului. Acestea două erau foarte populare în rândul studenţilor şi al tinerilor de pretutindeni, iar tinerii fanatici al-Qaeda nu făceau excepţie. Se pare că uşurinţa cu care pot fi folosite telefoanele mobile şi e-mailul, care le face atât de populare, creează de asemenea multe situaţii în care al-Qaeda este dirijată fără precauţiile OPSEC adecvate. Chiar dacă majoritatea sistemelor de e-mail pun la dispoziţie o criptare puternică, membrii al-Qaeda au fost prinşi folosind vechea criptare, mai slabă, de

doar 40 de biţi. Organizaţii precum ASN din America pot dezlega cu uşurinţă o astfel de criptare. Şi mai rău, cele mai multe e-mailuri ale al-Qaeda sunt trimise fără niciun fel de criptare.

Şi lucrurile devin şi mai rele. Membrii al-Qaeda sunt prinşi ducând agende cu adrese şi fişiere pentru computer care nu folosesc criptarea deloc. Dacă aceşti flăcăi se aşteaptă ca Allah să aibă grijă de nevoile lor de codare, poate ar trebui să li se spună că trec printr-o criză religioasă. Nu are sens să ai încredere în criptare atât timp cât nu o foloseşti. În Afganistan poate fi înţeleasă o asemenea neglijenţă, fiind o ţară unde au fost găsite o mulţime de materiale (drivere pentru hard disk, documente) în adăposturile al-Qaeda. Colapsul talibanilor a fost atât de rapid, încât ne-am putea aştepta ca în urma lor să fi rămas o mulţime de lucruri atunci când toată lumea s-a grăbit să scape. Este posibil ca şi religios să fi avut o legătură. Atunci când crezi că Dumnezeu este de partea ta, ai tendinţa să crezi că Domnul va avea grijă de tot (securitate pentru date şi orice altceva). Dar membrii al-Qaeda din afara Afganistanului ar fi trebuit să fie mai bine pregătiţi. Nu au fost.

„Antrenamentul terorist” oferit în Afganistan era de multe ori făcut la întâmplare şi concentrat mai mult pe îndoctrinarea militară, religioasă şi anti-Vest decât pe detaliile derulării unei operaţiuni secrete.

Probabil al-Qaeda nu ştia că în Pakistan exista un număr relativ restrâns de adrese de internet (IP), ţară care de altfel era locul preferat de grupare pentru a avea grijă de e-mailuri. Dacă înainte de septembrie 2001 SUA nu verificau fiecare element care provenea din conexiunile la internet ale Pakistanului, este foarte probabil ca începând de atunci să facă acest lucru. De fapt, se pare că a existat o monitorizare atentă a e-mailurilor şi operaţiunilor pe internet ale al-Qaeda înainte de 11 septembrie 2001, dar aceasta nu a putut surprinde elita agenţilor grupării. Deşi

aproximativ 20.000 de recruţi au trecut prin taberele de formare ale al-Qaeda între 1996 şi 2001, numai câteva sute au fost selectaţi pentru a fi agenţi de elită. Aceştia au acordat atenţie OPSEC-ului, sau cel puţin au făcut-o mai mult decât alţi agenţi cu funcţie inferioară. Aceşti agenţi de elită sunt cei care sunt căutaţi peste tot în lume. Unii au fost ucişi în luptele din Afganistan, alţii sunt încă în libertate în această ţară. Alţii sunt prizonieri în Afganistan şi în închisoarea Guantánamo.

Agenţii rămaşi, poate 100 – 200, se află în libertate în afara Afganistanului. Fără organizarea al-Qaeda din ţară, aceşti agenţi sunt pe cont propriu. Se pare că îi contactează pe absolvenţii mai puţin capabili ai grupării şi astfel unii dintre ei sunt prinşi din cauza folosirii neprecaute a emailului. Nu le sunt de ajutor nici miile de documente adunate în case abandonate, apartamente, tabere şi peşteri. Cu ajutorul acestora sunt identificaţi mulţi dintre cei care au fost în taberele de formare şi care se află acum în altă parte. Deşi agenţii al-Qaeda aflaţi în libertate sunt extrem de periculoşi, ei sunt de asemenea şi foarte vulnerabili, în mare parte, datorează acest lucru internetului.

CAPITOLUL 6 RĂZBOIUL INFORMAŢIONAL TERMENI TEHNICI

Glosarul complet, ce include şi termenii definiţi mai jos, poate fi găsit la sfârşitul cărţii.

Honey Pot – este un server instalat pe internet şi are unicul scop de a atrage hackeri. Odată ce aceştia găsesc serverul, ceea ce se întâmplă la câteva ore de la pornirea lui, detectorii de intruziune şi instrumentele de identificare, cu care este echipat Honey Pot, înregistrează tot ce fac hackerii atunci când încearcă să pătrundă. Astfel, hackerii *white hat* (tipii buni) află ce pun la cale hackerii *black hat* (tipii răi). Există o reţea numită Honey Net, între serverele căreia se face schimb de informaţii despre hackeri, informaţii ce sunt comunicate şi agenţiilor de securitate. Majoritatea acestor servere sunt conduse de voluntari care de multe ori suportă din propriul buzunar cheltuielile pentru întreţinerea lor.

Psyops – este prescurtarea de la operaţiuni psihologice. Jocul cu mintea inamicului. Cea mai simplă formă este lansarea unor fluturaşi deasupra trupelor inamice care explică de ce ar trebui să se predea, în formele mai sofisticate, sunt înfiinţate staţii radio pe care duşmanii le cred de partea lor, dar acestea transmit informaţii demoralizatoare.

PAO – este prescurtarea de la Public Affairs Officer[3]. Aceştia sunt cei care au de-a face cu mass-media. Fiecare forţă militară are angajaţi astfel de ofiţeri, întrucât mass-media a devenit o armă tot mai puternică.

Remailer – cunoscut şi sub numele de serviciu remailer anonim. Acesta este un site care ascunde orice informaţie despre e-mailul tău. Trimiţi e-mailul către remailer şi el îţi trimite o adresă anonimă, în unele cazuri, remailerul păstrează informaţii care, în cazul unui ordin

3 ofițer de relații cu publicul

judecătoresc, dezvăluie identitatea acelora care folosesc serviciul. Alte remailere distrug orice dovadă a adevăratei identităţi a utilizatorilor. Poliţia şi agenţiile antiteroriste nu agreează astfel de servicii, dar ele pot fi înfiinţate oriunde şi ar fi foarte dificil să fie înlăturate cu totul.

Deşi cyber-războiul este genul de luptă pe internet care îi sperie adeseori pe oameni, tindem să uităm că de fapt este un derivat al războiului informaţional. Informaţia este vitală pe internet, iar în războiul informaţional contează în primul rând cine controlează informaţia.

În vreme ce cyber-războiul se concentrează pe software şi hardware, războiul informaţional se referă la manevrarea informaţiilor. Adică de îndeplinirea scopului de controlare a informaţiei prin simpla ei manipulare. Cu toţii am auzit de „rotire". Gândeşte-te la războiul informaţional ca la o rotire a steroizilor utilizaţi de cineva. De ce să recurgi la cyber-război când există o cale mai simplă? De multe ori calea mai simplă trebuie combinată cu soluţii mai puţin convenţionale pentru a putea trimite un mesaj mai puternic. Cum spune zicala: „Când se sfârşesc cuvintele, armele vorbesc". Dar internetul permite mult mai multă vorbărie şi mult mai multe oportunităţi pentru a nu folosi altceva decât informaţii în declanşarea unui război. Internetul este cel mai rapid sistem de comunicaţii inventat vreodată. Oricine îl poate folosi, păstrându-şi anonimatul. Războiul informaţional nu va mai fi niciodată la fel şi internetul este motivul principal pentru acest lucru.

Un exemplu recent a avut loc în timpul Războiului din Afganistan, când opinia publică din ţările musulmane era în mare parte controlată de terorişti şi adepţii lor. Zvonurile şi minciunile sfruntate (dar cu priză la public) erau folosite pentru a convinge o mare parte a musulmanilor că atacurile de la 11 septembrie au fost un complot israelian, iar „războiul împotriva terorismului" era o scuză pentru un război împotriva islamului. Internetul a

jucat un rol major în acest război al minciunilor şi al răsturnărilor de situaţii.

INFORMAŢIA ESTE FUNDAMENTALĂ

Informaţia şi utilizarea ei în luptă sunt fundamentale pentru războiul informaţional. De multe ori, acesta nu presupune decât obţinerea şi analizarea mai rapidă a informaţiilor cu ajutorul computerelor.

De exemplu, în anii ’70, serviciul forestier american a organizat o activitate pentru prevenirea incendiilor din pădure. Ideea de bază era că incendiile sunt destul de predictibile dacă primeşti un flux constant de informaţii despre o zonă cu privire la condiţiile meteo (viteza şi direcţia vântului) şi tipul de copaci şi vegetaţie, umezeală etc. Această activitate îţi permitea să avansezi supoziţii pornind de la informaţiile tale pentru a preveni izbucnirea focului. Ceea ce s-a demonstrat la final a fost că erau nevoiţi să îşi îndrepte eforturile spre locurile cu cea mai mare posibilitate de izbucnire a unui incendiu şi nu acolo unde aveau loc deja. Nu era vorba decât despre a făcu un pas înaintea focului pentru a-ţi putea folosi resursele limitate (pompieri şi echipament) pentru a-l opri. Instrumentele războiului informaţional îţi permit să vezi viitorul mai rapid şi mai corect decât oponentul tău. Toţi cei implicaţi în piaţa acţiunilor duc un război informaţional. Dacă nu lucrezi cumva pe Wall Street, unde eşti mult mai aproape de informaţiile importante despre acţiuni, te afli în dezavantaj. Cel care are cele mai bune informaţii va face mai mulţi bani, de multe ori pe spinarea celor care nu ajung la ele la fel de repede.

Serviciul forestier a introdus în calculator aceste simulări de prevenire a incendiilor şi s-a folosit de foarte multă tehnologie în lupta cu focul. Printre dispozitivele folosite se numărau camere video aeropurtate pentru a urmări avansarea focului şi condiţiile vremii (intensitatea şi direcţia vântului, umiditatea, detalii care fac diferenţa

atunci când lupţi cu incendii de mare amploare). Există multe asemănări între lupta cu focul şi lupta cu un adversar. Dar există şi o diferenţă importantă. Incendiile sunt o forţă a naturii care urmează legile naturii. Adversarii umani sunt mai puţin previzibili, pentru că ei pot raţiona, în vreme ce focul nu poate face asta. Aici se află una dintre posibilele probleme ale războiului informaţional.

Atunci când ai multe date despre un incendiu, poţi prevedea, cu un mare grad de probabilitate, cum va evolua acesta. Mai mult, modelul computerului poate furniza o predicţie corectă despre evoluţia focului dacă sunt folosite diferite strategii pentru a-l opri în următoarele ore sau zile. Astfel, controlul asupra informaţiei îţi permite să ai o mai bună imagine asupra viitorului.

Dar atunci când oponentul tău este uman, lucrurile devin mai puţin previzibile. Un incendiu se deplasează în direcţia în care bate vântul şi în funcţie de teren (copaci sau desişuri nearse). Dar un adversar uman va încerca să te ia prin surprindere. Aici intervine internetul. De multe ori există probleme tehnice cu internetul şi cu numeroasele reţele mai mici conectate la el. Componentele hardware se strică, iar programele au erori. Dacă ar fi numai asta, tehnicienii ar putea depista rapid problemele şi le-ar rezolva. Dar dacă, aşa cum se întâmplă din ce în ce mai des, o problemă de pe internet este rezultatul încercării unui hacker de a strica ceva? Ca să îţi dai seama dacă acea problemă provine de la hardware-ul sau software-ul stricat ori de la atacul unui hacker, trebuie să ai suficiente informaţii despre ce se petrece. Un hacker bun se va proteja făcând ca pagubele produse de el să pară lucruri „normale” (hardware sau software avariat).

Adversarii se dau peste cap pentru a-i împiedica pe ceilalţi să adune informaţii. Un duşman pe câmpul de luptă va încerca şi îţi va furniza date eronate. Ţinând cont de toate acestea, este logic ca utilizarea mai multor

computere, a comunicaţiilor de mare viteză (telefoanele mobile) şi a sateliţilor pentru operaţiuni de luptă să fie numită război informaţional. Pe vremuri, acest joc era numit, simplu, înşelătorie. Dar cu internetul, cantitatea şi viteza informaţiilor din jurul nostru sunt mult mai mari. Este o cu totul altă lume.

Internetul este cel mai avansat câmp de luptă pentru acest tip de război. Cu fiecare lună care trece, tot mai multe lucruri sunt disponibile pe net. Cum scopul războiului a fost întotdeauna distrugerea abilităţii duşmanului de a mai putea lupta, internetul se transformă într-un important câmp de luptă. Dar asemenea câmpurilor de luptă tradiţionale, internetul este plin de civili. Adică noi, utilizatorii simpli! Şi ştii ce se întâmplă cu civilii prinşi în luptă. Cyber-războinicii, la fel ca toţi soldaţii din toate războaiele, vor fi preocupaţi în primul rând de îndeplinirea misiunii. Dacă un număr mare de utilizatori civili sunt deconectaţi, sau le sunt implicate PC-urile în tot acest proces... ghinion! Pentru cyber-războinici, viteza în îndeplinirea misiunii este mai importantă decât orice altceva. Dacă se mişcă prea încet, adversarii îşi vor întări apărarea şi vor fi primii care îţi vor distruge resursele. Războiul informaţional nu are în vedere numai informaţia, ci şi viteza şi distrugerea celuilalt înainte de a te repera.

ÎNŞELĂTORII

Nu uita niciodată că cele mai bine echipate arme electronice pot fi înfrânte prin contramăsuri destul de simple. Cei din forţele aeriene americane sunt încă frustraţi de modul în care au fost duşi de nas prin păcăleli ieftine în Kosovo şi Irak. De-a lungul anilor ’90 am lansat bombe în Irak şi existau preocupări dacă acestea ating ţintele vizate. Dar chiar şi înainte de evenimentele din Irak, forţele aeriene se confruntaseră îndelung cu astfel de înşelătorii în Coreea, la începutul anilor ’50, fapt care s-ar putea repeta acum, la mai bine de 50 de ani.

După sfârşitul Războiului Rece, CIA a publicat rapoarte detaliate despre înşelătoriile din China şi Coreea de Nord împotriva militarilor americani din timpul Războiului din Coreea (1950 – 1953). Timp de trei ani, America a încercat în zadar să întrerupă aprovizionarea trupelor comuniste de-a lungul liniei de front din Coreea centrală. O mare parte a acestui eşec s-a datorat unei strategeme simple şi de succes a comuniştilor. Podurile, care de sus păreau bombardate, erau reparate în moduri care încă permiteau folosirea lor (fie şi numai pe timpul nopţii), în vreme ce de sus păreau impracticabile. O altă tehnică de înşelare preferată era echiparea camioanelor cu butoaie pline cu cârpe uleioase sau paie. Când avioanele americane atacau convoiul, se dădea foc butoaielor fie că fusese lovit sau nu vreun camion, producând astfel un fum dens. Şoferii erau apoi instruiţi să iasă de pe şosea şi să părăsească maşinile. De sus, piloţii, încântaţi de precizia lor, plecau în căutarea altor ţinte. Odată cu dispariţia avioanelor inamice, butoaiele erau acoperite cu capace pentru a opri focul şi convoiul mergea mai departe. Câteva camioane tot ar fi putut fi lovite, dar nu la fel de multe ca în cazul în care avioanele ar fi trimis bombe neîncetat.

Forţele aeriene susţin că pot învinge aceste trucuri vechi de jumătate de secol cu senzori mai buni (camere video de o mai mare precizie). Poate, dar asta în cazul în care comuniştii nu şi-au actualizat acele trucuri în ultima jumătate de secol. Este puţin probabil ca avioanele de război să fie superioare din acest punct de vedere. Forţele aeriene nu au fost capabile să-i împiedice pe sârbi să-şi aprovizioneze trupele în Kosovo, în 1999. Americanii au crezut că au folosit cu succes puterea aerului pentru a opri forţele irakiene în Kuweit în 1991. Totuşi, mai târziu s-a descoperit că majoritatea acelor trupe erau formate din kurzi şi şiiţi, exact genul de oameni de care dorea Saddam să scape. Chiar şi în vremurile cele mai bune, el nu aproviziona cum se cuvine aceste trupe şi nu era interesat

să depună eforturi (precum înşelătoriile) pentru a le trimite în continuare hrană şi apă în deşertul kuweitian. De fapt, aceste trupe nu numai că îşi primeau proviziile, ci şi beneficiau de permisii. Trupele de la sol au găsit întotdeauna metode simple de a evita să fie lovite de avioanele de luptă. Nu ar trebui să ne surprindă, întrucât acestea fie veneau cu astfel de soluţii bune, fie mureau. S-a dovedit a fi un foarte eficient program de motivare.

Situaţia este mai rea decât pare, pentru că forţele aeriene nu au luat niciodată destul de în serios aceste trucuri de la sol pentru a depune un efort însemnat de evitare a lor. Nu există un motiv raţional pentru acest lucru care are loc de mai bine de 60 de ani. Şi asta nu numai în cadrul forţelor aeriene americane, ci şi ale altor naţiuni. Aşadar, seria „Ups, avem o problemă" este foarte probabil să continue şi în epoca cyber-războiului.

Există deja indicii că acest tipar este urmat. Conceptul de *Honey Pot-uri* (servere setate să arate ca nişte ţinte interesante, care atrag şi distrag hackerii talentaţi de la ţintele reale) este deja folosit. Multe firewall-uri şi alte programe de securitate folosesc de asemenea forme de a păcăli pentru a ţine la depărtare pagubele serioase pe care hackerii le-ar putea face. Pe lângă instrumentele de cyber-război ofensive, niciun apărător nu duce lipsă de tehnici pentru a bara atacurile. Administratorii de sistem, la fel ca infanteria inamică ce încearcă să evite bombardamentul, sunt foarte motivaţi să găsească o cale pentru a-şi păstra sistemele în funcţiune. Hackerii cred că totul este sub control, întrucât pot alege când şi unde să atace. Iar mass-media tinde să dea curs atacurilor reuşite ale acestora, mai degrabă decât celor care eşuează deşi sunt mai frecvente. Un vechi adevăr universal militar spune că pentru fiecare ofensivă există o defensivă care, de obicei, are mai multe şanse de izbândă.

VICTIMELE PSIHOLOGICE ALE CYBER-

RĂZBOIULUI

Războiul informaţional şi cyber-războiul au deschis noi oportunităţi pentru forme de luptă mai vechi şi, într-o oarecare măsură, mai exotice. Un aspect al războiului cunoscut de multă vreme, dar folosit destul de rar sunt operaţiunile psihologice *(psyops).* Este vorba de jocul cu mintea inamicului. Considerat atrăgător şi intens discutat, războiul psihologic nu este pus în practică atât de des pe cât te-ai aştepta. Există câteva motive pentru care *psyops*-urile nu au fost folosite mai des sau de ce au succes atunci când intră în joc. În primul rând, *psyops-ul* este înfricoşător (se poate întoarce împotriva utilizatorului în mod perfid) şi apoi este puţin înţeles de majoritatea liderilor militari. Şi chiar dacă ar fi înţeles, este de multe ori dat la o parte din cauza unor chestiuni vitale (precum logistica, operaţiuni de luptă şi comunicaţii cu aliaţi şi lideri politici). Mai mult, domeniul a devenit mai complex de-a lungul secolului XX. Acum avem războiul informaţional (mass-media şi jocurile electronice), afacerile publice (relaţiile cu mass-media la un nivel profesionist), dar *şi psyops.* Asta înseamnă că acum dispui de trei birocraţii militare care se luptă pentru a şti cine ce face, de cele mai multe ori folosind aceleaşi resurse. De exemplu, susţinătorii *psyops* au descoperit că aeronava pentru *psyops* a Comandamentului Solo al forţelor aeriene americane (aparat de zbor care poate difuza semnale radio şi TV) nu are suficient de mult semnal pentru a influenţa operaţiunile în mod decisiv. Acest lucru s-a descoperit în Balcani în timpul manevrelor din Kosovo, în 1999. Acum, cel puţin, nu trebuie să se mai lupte cu oamenii războiului informaţional pentru conducerea Comandamentului Solo. Atât *psyops,* cât şi războiul informaţional vor acces la sateliţi pentru a difuza semnale cât mai puternice. Mai întâi trebuie să îi convingă pe statisticieni că mesajul lor merită cheltuielile mari pentru transport.

Încă se mai analizează deciziile cu privire la oamenii

noului război informaţional şi ce poate face echipa *psyops.* Profesioniştii războiului informaţional au început prin înşelătorii pe internet şi rotiri politice. Cei care susţin acest război sunt un fel de combinaţie între maniaci ai internetului şi oameni care au lucrat pentru CIA şi departamente de stat. Apoi mai sunt şi funcţionarii afacerilor publice, care transmit informaţiile oficiale presei. De multe ori, cei din *psyops* şi din războiul informaţional vor să preia controlul asupra declaraţiilor oficiale (înserarea unor detalii pe jumătate adevărate sau a unor minciuni sfruntate) ca parte a unei stratageme. Dacă fac acest lucru, îi discreditează pe cei de la afaceri publice. Acestora din urmă le place să fie în relaţii bune cu jurnaliştii, în vreme ce *psyops-ii* şi războinicii informaţionali sunt puţin interesaţi de asta. Tot acest zbucium interior şi această confuzie stă în calea realizării oricărui lucru. Nu este foarte clar dacă situaţia se va îmbunătăţi în viitorul apropiat.

Internetul a creat multe noi oportunităţi pentru *psyops.* Din păcate, multe dintre ele nu sunt folosite de profesioniştii din domeniu (care preferă vechile tehnici precum aruncarea din aer a fluturaşilor şi înfiinţarea de staţii radio). Internetul furnizează mijlocul perfect pentru a agita lucrurile în privinţa oricărei idei sau cauze pe care cineva vrea să o urmeze. A durat ceva vreme până când activitatea internetului a fost constant conectată la radio, TV şi publicaţiile mass-media. Dar încă de la mijlocul anilor ’90, jurnaliştii din presa scrisă şi electronică au început să vadă internetul ca pe o sursă de informaţii captivante (chiar dacă nu mereu corecte). Ca întotdeauna, aceia care au talentul de a spune ceva potrivit, în modul potrivit, la momentul potrivit, publicului potrivit pot atrage atenţia oamenilor. Totul ţine de faptul că poţi face toate astea mult mai repede şi mai ieftin prin transmiterea mesajului (adevărat sau fals) pe web, cu viteza luminii.

Până acum, cei cu un talent adevărat pentru acest tip

de război psihologic pe internet o fac numai din motive comerciale. Vânzarea filmelor, a muzicii sau a orice altceva pe internet s-a dovedit a fi foarte eficientă. Este ieftin, ceea ce înseamnă că nu îţi asumi riscuri prea mari. Şi dacă funcţionează, ajungi să câştigi mult mai mult decât ai investit.

Psyops-urile pe internet vor ajunge probabil în atenţia tuturor numai atunci când va exista cu adevărat un cyber-război. Într-o astfel de situaţie, poţi adăuga panică şi demoralizare efectelor cauzate de distrugerea serverelor şi a reţelelor. O simplă informaţie greşită, şi victimele îşi vor repune sistemele mai încet în funcţiune. Pentru a face asta, trebuie să semeni o temere convingătoare, nesiguranţă şi îndoială cu privire la internet şi toate astea într-un timp scurt. Cu cât este cineva mai convingător, cu atât mai mult le va lua victimelor să îşi dea seama că sunt trase pe sfoară.

Este o armă puternică. Din păcate, numai puţini militari şi-au dat seama cum să o folosească în mod corect. Şi asta pentru că, spre deosebire de civili (numiţi afectuos „informatori comerciali"), militarii nu au parte de prea multă practică. Ai nevoie de rezultatele unei acţiuni reale pentru a vedea ce funcţionează sau nu. Civilii au parte de practică şi astfel sunt mult mai eficienţi. Poate că cea mai bună metodă este recrutarea cât mai multor astfel de civili şi eliberarea lor pe timp de război.

RĂZBOIUL INFORMAŢIONAL ŞI COMPETENŢA PAO

În mod tradiţional, cea mai mare parte a eforturilor militare într-un război informaţional este direcţionată împotriva jurnaliştilor. Arma-cheie pentru armată sunt funcţionarii PAO. Ei sunt cei cu care au de a face jurnaliştii. Fireşte, nu toate ţările sau serviciile din forţele armate ale unei naţiuni sunt la fel de eficiente. Un studiu din anul 2000 făcut de 92 de jurnalişti (care de obicei se

ocupă de probleme de apărare) a dezvăluit că ofiţerii de afaceri publice ai forţelor aeriene americane sunt cei mai competenţi. La mică distanţă se aflau cei de la infanterie, care erau consideraţi cei mai cooperativi şi mai credibili. Flota maritimă era pe locul al treilea, iar pe ultimul se aflau ceilalţi militari. Aceasta este singurul serviciu care nu are PAO ca domeniu de activitate separat, în schimb, are ofiţeri de frunte, cărora le oferă un scurt instructaj (despre cum să relaţioneze cu mass-media) şi, timp de câţiva ani, trebuie să întreţină relaţiile cu presa. Armata şi-a dat în cele din urmă seama că acest lucru nu prea dă roade şi a creat posturi PAO.

RĂZBOI INFORMAŢIONAL PENTRU MAI MULŢI BANI

Una dintre aplicaţiile militare ale actualului război informaţional se află chiar în ograda noastră. De la sfârşitul Războiului Rece din 1991, Pentagonul a fost scena unei lupte publicitare aprige între forţele aeriene, flotă şi marină. Toate aceste servicii americane se luptă pentru imaginea de forţă combativă a viitorului. În mod special, toate susţin că pot duce viitoarele războaie ale Americii cu cea mai mare eficacitate şi cu un cât mai mic număr de victime. Speră că tehnologia le va putea conferi supremaţie. Până acum, forţele aeriene sunt cele care sunt primele. Avioane cu reacţie arătoase şi bombardiere secrete, care folosesc aparate electronice strălucitoare şi bombe inteligente ce generează imagini pe placul mulţimii. Armata a răspuns cu noi detaşamente, mai uşor de transportat (către locuri fierbinţi aflate la distanţă), care folosesc maşini blindate în locul tancurilor mult mai grele. Deşi flota nu a venit cu ceva care să-ţi ia ochii, toate ramurile se luptă pentru o mai mare parte din bugetul pentru apărare, dar şi pentru supremaţie în modul în care vor fi purtate războaiele viitoare.

Forţele aeriene, de exemplu, merg pe aceeaşi linie pe

care au mers în ultimii 60 de ani: putem face totul din aer. Acest concept nu a dat mereu roade după cel de-al Doilea Război Mondial, dar cu toate acele avioane moderne şi tehnologia asociată, forţele aeriene au putut convinge publicul de eficienţa lor. Nu va fi aşa, iar atunci când trupele armatei şi ale marinei, slab subvenţionate, vor trece la treabă pentru a „face curat” (cum le place forţelor aeriene să spună), trupele de la sol vor fi anihilate. Forţele aeriene au succes pentru că întotdeauna intervin în orice operaţiune militară. Un astfel de caz a fost Războiul din Afganistan din 2001. Utilizarea puterii aerului împotriva membrilor triburilor bine înarmaţi a fost impresionantă, dar nu era nimic nou de vreme ce englezii au făcut şi ei acelaşi lucru cu irakienii în anii ’20. Acest lucru scoate în evidenţă o altă armă din arsenalul războiului informaţional: uitarea trecutului. Sau mai important decât atât, ai grijă ca nimeni să nu aducă în prim-plan momente stânjenitoare din trecut. Hei, istoria este plictisitoare. Aşa cum a spus consacratul istoric şi producător de avioane, Henry Ford, „Istoria este un nonsens”. Aminteşte-ţi ce a spus un alt om de seamă din trecut (şi primul general care a folosit puterea aerului utilizând baloanele cu aer cald), Napoleon Bonaparte: „Istoria este minciuna cu care toată lumea este de acord”. Dar istoria are obiceiul urât de a-ţi da o palmă peste faţă atunci când te aştepţi mai puţin.

Partea proastă este că toţi iau totul de-a gata. În PR, încrederea şi consecvenţa sunt fapte bune care nu trec nepedepsite. Gloria ajunge în lumina reflectoarelor, nu lucrul cel mai eficient. Războiul informaţional ţine în primul rând de înşelătorii. Şi atunci când ajungi să crezi în articolele de presă scrise despre tine, ai dat de bucluc.

CITIREA E-MAILURILOR ALTORA.

Războiul informaţional nu are loc numai între naţiuni. Are loc şi între organizaţii mai mici sau chiar indivizi. Acest tip de război de mare viteză a început odată cu

reţelele de telegraf din secolul al XIX-lea şi cu dezvoltarea rapidă a reţelelor telefonice de la începutul secolului XX. La începuturile internetului, vrajba dintre cei care duceau un război informaţional, un cyber-război, nu era ceva neobişnuit. Primii hackeri erau individualişti, dar tindeau să acţioneze în văzul tuturor. Nu existau prea multe mârşăvii pentru simplul motiv că toată lumea avea acces cam la aceleaşi instrumente şi accesul la „programele" din vremea aceea era liber pentru toată lumea. Dacă făceai ceva nelalocul lui, erai descoperit repede şi tras la răspundere. Această perioadă s-a terminat în 1988, odată cu apariţia primului remailer anonim. Era un program pentru internet care ascundea identitatea utilizatorilor. La început, aceste remailere au fost create şi date în folosinţă pentru ca oamenii să poată discuta liber subiecte sensibile sau tabu (precum abuzurile sexuale împotriva minorilor sau alte obiceiuri ciudate). Deşi unii au anticipat o invazie de mesaje calomnioase sau maliţioase din partea acestor noi utilizatori anonimi, acest lucru nu s-a întâmplat niciodată. S-au înregistrat abuzuri, dar nesemnificative.

Dar „minor" este relativ. Utilizarea remailerelor de către indivizi nu a fost niciodată o problemă demnă de remarcat Dar campaniile anonime de tipul războiului informaţional, bine organizate, erau ceva cu totul diferit. Fraudele pe piaţa de schimb prin majorarea valorii acţiunilor folosind mesaje anonime (şi apoi vânzarea acţiunilor înainte de dezvăluirea adevărului) încă mai au loc. Cu toate că autorităţile îi prind de cele mai multe ori pe făptaşi şi îi judecă, lucru care pe unii îi descurajează, oamenii continuă să umfle preţurile în mod artificial. Există şi trucuri legale, cum ar fi postarea de comentarii elogioase pe internet despre un nou CD de muzică, un film sau o carte. Nu este tocmai ilegal, dar nici etic nu este. O astfel de activitate este numită „comercializare virală" (ca în cazul unui virus care se răspândeşte peste tot pe internet). Modul în care a fost comercializat filmul cu

buget scăzut *The Blair Witch Project* pe internet este considerat unul dintre cele mai bune exemple de acest fel.

Utilizatorii de internet sunt mai puţin anonimi decât îşi închipuie, lucru ce a dus la multe încercări de fraudare din partea celor care sunt rapid localizaţi şi depistaţi de către cei mai experimentaţi şi de FBI. Dar sunt multe cazuri în care aceştia chiar au un anumit grad de anonimitate. Atunci când te afli pe un chat, numele pe care îl foloseşti nu înseamnă de obicei nimic, dar se poate afla ce adresă IP foloseşti. De fiecare dată când te conectezi la internet ai nevoie de o adresă IP (un fel de număr de telefon al internetului). Dacă formezi numărul printr-un modem, ISP-ul îţi va furniza automat o adresă IP din mulţimea de adrese alocabile. Dacă foloseşti ISDN sau un modem prin cablu, vei avea probabil propria adresă IP, unică. De obicei e nevoie de un ordin judecătoresc sau de o investigaţie a poliţiei pentru a afla numele şi adresa ataşate unui IP. Deci dacă activităţile tale pe internet sunt inocente, ai un anumit grad de anonimitate. Dacă treci linia spre activităţile ilegale, vei ieşi cu siguranţă din anonimat.

S-a dezvoltat o cultură ce încurajează oamenii să spună lucruri pe care în mod normal nu le-ar spune cuiva în faţă. Îi afectează pe toţi, indiferent de vârstă, sex sau statut social. În multe cazuri, ca în grupurile de ştiri sau pe forumuri, un astfel de comportament exuberant este o mică plăcere şi nu o problemă. Se transformă însă într-una atunci când exuberanţa trece în e-mailuri. Nu este vorba de mailurile private, ci de cantitatea tot mai mare a celor trimise prin intermediul conturilor companiilor şi guvernului. Utilizatorii au descoperit, deloc uşor, că regulile pentru emailul personal şi cel comercial sunt foarte diferite. Motivul este simplu. Când cineva spune ceva prin mailul personal, vorbeşte în numele lui. Când spune acelaşi lucru folosind contul de la locul de muncă, se subînţelege că vorbeşte în numele organizaţiei. După ce au

fost intentate câteva procese în anii ’90, s-a stabilit că acel cont de e-mail al companiei sau organizaţiei la care lucrezi îţi este dat în folosinţă, nu în proprietate. Organizaţia este cea care îl deţine şi are control asupra a ceea ce se întâmplă cu el.

Această grabă a organizaţiilor de a dezvolta reguli pentru folosirea e-mailului nu a apărut numai din cauza celor obsedaţi de controlul companiei sau de avocaţi. Dacă un om spune ceva nepotrivit prin contul de e-mail al companiei, compania poate fi dată în judecată. Dar lucrurile au mers şi mai rău. Avocaţii care dădeau în judecată companiile pentru chestiuni nelegate de e-mail au descoperit că aceste e-mailuri noi conţin adesea declaraţii compromiţătoare pe care rareori le găseau în corespondenţa scrisă. Din nou, există acea concepţie că ceea e spui pe e-mail este cumva mai puţin durabil sau îţi creează mai puţine obligaţii decât ceea ce ai trimis printr-un poştaş sau ai distribuit local, unui cerc restrâns de persoane. Mai mult, e-mailurile de afaceri sunt salvate în mod constant de cele mai multe companii. Astfel, chiar dacă un angajat a şters documente electronice, avocaţii înverşunaţi le pot recupera mai târziu de pe casetele de rezervă ale departamentului IT.

Ceva trebuia făcut; e-mailul trebuia îmblânzit. Tehnologia a fost pusă în serviciul îmblânzirii… tehnologiei. Monitorizarea software-ului este inclusă în prezent la locul de muncă pentru a urmări ce fel de e-mailuri trimit şi primesc utilizatorii. Cu toate că armata americană monitorizează de multă vreme toate mesajele care vin şi pleacă de pe adresele „mii”, astfel de sisteme devin tot mai populare în toate tipurile de companii sau armate străine pentru a căuta anumite cuvinte sau expresii ce ar putea indica mesajele nepotrivite. Nu numai limbajul neadecvat este criticat, dar şi discuţiile neautorizate despre materiale secrete şi indicii de neloialitate. Teama de terorism din SUA face acest lucru să fie tot mai des

întâlnit şi, fără îndoială, se va răspândi.

E-mailul (şi chiar şi chatul) care monitorizează software-ul întrece uneori măsura. Corectitudinea politică sau doar atitudinea foarte conservatoare cu privire la „limbajul acceptabil” îi deranjează pe mulţi angajaţi care se trezesc că un mail trimis ce conţine cuvântul „căţea” (cu referire la o discuţie despre creşterea câinilor de vânătoare de rasă) le este imputat ca „limbaj inacceptabil”. Însă mulţi nu îşi dau seama că acelaşi tip de tehnologie va fi în curând folosit pentru monitorizarea apelurilor telefonice efectuate de pe telefoane mobile.

Legea americană a protejat pentru multă vreme dreptul organizaţiilor de a ţine evidenţa înregistrărilor proprii (corespondenţa a fost considerată mult timp o „evidenţă a companiei”) departe de ochii iscoditori şi sub controlul funcţionarilor corporaţiei. Apariţia şi popularitatea emailului au adus noi oportunităţi. În trecut era plictisitor pentru un manager să recitească toate documentele pe care le emitea compania. De multe ori, necazurile cel mai mari apăreau din cauza unor informaţii despre care nu ştia nimeni nimic. În orice caz, după ce avocatul celeilalte părţi termina de săpat printre tonele de memorandumuri şi corespondenţă, apăreau de obicei destul de multe dovezi incriminatorii.

Nu acelaşi lucru se întâmplă cu documentele electronice şi e-mailurile. Liderii companiilor şi-au dat repede seama nu numai că pot monitoriza documentele şi mesajele emise de organizaţia lor, dar şi că în numai câteva minute pot verifica eventuale comportamente nelalocul lor. Pentru companiile cinstite, şi majoritatea sunt cinstite, această epocă a documentelor electronice linişteşte lucrurile şi îngreunează comiterea de ilegalităţi (nedescoperite). Deşi este adevărat că există firme ce vând software care garantează „tocarea” documentelor electronice, încă se mai păstrează copii de rezervă, iar unele mesaje sunt reperate şi salvate în locaţii ce nu sunt

la îndemână. Oamenii de afaceri necinstiţi şi oficialii guvernamentali ar prefera ca e-mailul să dispară, dar este puţin probabil ca asta să se întâmple. Oricine arată vreo preferinţă pentru a comunica numai faţă în faţă sau prin telefon este tot mai des privit cu suspiciune (şi probabil este considerat un ignorant în ceea ce priveşte tehnologia prin cablu).

Încă mai există o mulţime de documente tipărite, dar tendinţa este de a le scana pe cele care trebuie salvate pentru evidenţele electronice. Astfel este ocupat mai puţin spaţiu, există un pericol de incendiu mai redus, iar formatul este mai uşor de utilizat. În mod ciudat, această utilizare a documentelor electronice nu a dus la promisul „birou fără hârtii”. Dimpotrivă, oamenii tipăresc multe dintre documentele electronice fie pentru că le este mai comod să citească de pe hârtie şi nu de pe monitor, fie pentru că li pare mai sigur să aibă şi un document tipărit. De fapt, copia electronică este mai sigură, mai uşor de găsit şi cu o durată de viaţă mai mare.

RĂZBOIUL INFORMAŢIONAL INTERN

Nu toţi războinicii informaţionali se concentrează pe inamic. Versiunea militară a „politicii de birou” s-a desfăşurat chiar şi în timpul Războiului din Afganistan sau, mai bine spus, din cauza lui. Cei din forţele aeriene erau supăraţi că nu participă decât la o mică parte din acţiune (au parte de articole de ziar favorabile) în prima etapă a războiului, în prima lună, de exemplu, în unele zile erau aruncate numai câteva bombe asupra Afganistanului, dar erau până la 80 de avioane ale flotei care operau. Flota se asigura că jurnaliştii vin la sediile ei unde aveau prilejul de a filma cum decolează avioanele de război. Au fost realizate numeroase interviuri cu marinari şi aviatori. Părea că flota duce singură lupta de deasupra Afganistanului.

Forţele aeriene aveau un mare dezavantaj întrucât nu

aveau baze suficient de aproape de Afganistan pentru cea mai mare parte a avioanelor de război. Unele aeronave uşoare de tip AC130 şi F-15 au început să opereze din baze din Golful Persic, dar naţiunile implicate nu doreau să facă acest lucru public. Şi asta pentru că toată propaganda antiamericană ce circula pe internet şi prin alte mijloace media i-a făcut pe arabii de condiţie medie să fie fermi împotriva americanilor. Forţele aeriene au lansat atacuri de la o bază din insula engleză pe care o controlau, Diego García, din Oceanul Indian. De fapt, erau lansate de două ori mai multe bombe decât în mod obişnuit, dar nici măcar acolo forţele aeriene nu au beneficiat de publicitate, întrucât englezii nu permiteau accesul reporterilor pe insulă; locuitorii fuseseră evacuaţi cu mulţi ani înainte, atunci când insula a fost transformată în bază militară; astfel nu exista nimeni care să poată fi mituit pentru a stoarce informaţii.

Forţele aeriene nu au putut agita apele pentru a aduce în lumina reflectoarelor impactul decisiv al bombardierelor trimise asupra Afganistanului. Acest lucru ar putea avea consecinţe serioase într-un viitor război, pentru că numai acele câteva bombardiere (16 aeronave B-1 şi B-52 au lansat două treimi din bombe) erau mult mai eficiente decât mai multe sute de avioane de război care operau de la bază. Totuşi, flota încă îşi mai foloseşte maşinăria de PR pentru a se asigura că în următorii zece ani primeşte mai mulţi bani pentru baze, în detrimentul forţelor aeriene. De fapt, forţelor aeriene le-ar plăcea să construiască bombardiere cu o rază de acţiune mai mare, dar ar prefera să creeze avioane de luptă cu bătaie scurtă. În zece ani, rezultatele acestei dispute pot fi o chestiune crucială pentru americani.

RĂZBOIUL INFORMAŢIONAL TELEVIZAT

Unul dintre aspectele mai puţin înţelese dar destul de importante ale războiului informaţional de la începutul

secolului XXI este rolul jucat de mass-media americană. Mai exact, este vorba de impactul global pe care filmele şi emisiunile de televiziune americane îl au din cauza modului în care înfăţişează Statele Unite şi pe americani. Ce are de a face acest lucru cu cyber-războinicii şi lupta dusă pe internet? Chiar foarte multe. Străinii (ca de altfel şi majoritatea americanilor) îşi formează o mare parte din impresiile despre cyber-război şi cyber-războinici prin intermediul mass-media (şi al numeroaselor filme şi emisiuni TV americane care le prezintă). La sfârşitul secolului XX, atunci când războiul informaţional a devenit un instrument militar în toată regula, Departamentul Apărării a început să acorde atenţie modului în care era prezentat spaţiul cibernetic.

Armata a avut o îndelungată relaţie cu producătorii de film, mai ales pentru ca filmele cu subiect militar sunt mai ieftine deoarece Departamentul Apărării cooperează şi furnizează echipament militar gratuit sau pentru sume modice. Evident că armata nu ar fi oferit aceste lucruri pentru un film care să o pună într-o lumină proastă. Nimeni nu s-a gândit la acest aspect ca parte a războiului informaţional până în anii ’90; era vorba doar de un PR bun. Dar există o diferenţă între a păstra o imagine bună într-un film şi un război informaţional propriu-zis. De exemplu, un număr de filme şi de emisiuni americane despre participarea SUA în Vietnam au lăsat impresia că aproape toţi soldaţii americani au fost eficienţi şi nu agreau războiul. Dacă ne uităm pe orice declaraţie despre acel episod, vedem că lucrurile au stat exact pe dos. Acest lucru le-a dat impresia unora precum Saddam Hussein sau Osama bin Laden că, orice ar face, America nu va veni sau nu va putea veni după ei pentru că îi este teamă să îşi asume victimele. Lumea ar fi fost un loc mai bun dacă aceştia doi s-ar fi gândit mai bine la ce avea să se întâmple dacă sfidează forţele armate americane.

Încă de la sfârşitul anilor ’90, Departamentul Apărării

s-a implicat mult mai activ în controlul modului în care producătorii de televiziune prezintă guvernul. Deşi se ştie că filmele americane rulează peste tot în lume, emisiunile de televiziune americane sunt difuzate la o scară încă şi mai mare. Astfel acum se acordă o mai mare atenţie modului în care arată trupele la televizor. De exemplu, la sfârşitul anului 2000, serviciile secrete au făcut cunoscut că sunt nemulţumite de felul în care emisiunea *DAG* a postului NBC le-a prezentat ca fiind incapabile să păzească o primă doamnă imaginară. Serviciile secrete se temeau cel mai rău ca nu cumva unor răufăcători să le vină ideea de a ataca pe cineva dintre cei protejaţi de servicii.

Producătorii popularului serial de la NBC, *Viaţa la Casa Albă,* voiau de fapt să prezinte o versiune diferită asupra aceleiaşi teme într-un show realizat la Pentagon. Noul program nu a mai fost început, dar Departamentul Apărării l-a văzut ca pe o oportunitate pentru a apărea fie într-o lumină proastă, fie într-una bună.

Uneori şi să dai bine poate fi o problemă. În 2001, o companie de producţie TV a anunţat că va realiza o emisiune numită *Combat Missions*. În această serie, echipe de foşti sau actuali luptători de comando (din forţe speciale, SEALS, poliţie, SWAT, DEA, FBI, rangeri etc.) vor concura pentru îndeplinirea unor misiuni militare. Departamentul Apărării a interzis imediat celor încă activi să participe. Motivul era unul practic: serialul avea să se concentreze pe acrobaţii captivante şi nerealiste care în filme sunt luate ca fiind operaţiuni militare. De când filmele au început să îi prezinte pe soldaţi făcând fapte eroice nerealiste, generaţii de instructori au trebuit să îi convingă pe tinerii recruţi că dacă vor face lucrurile în acel mod, vor muri foarte repede. Timp de mai multe decenii, astfel de sergenţi au strigat: „Nu vreau să aud prostii în genul lui John Wayne!” În ultimele două decenii, strigătul a sunat de obicei cam aşa: „Nu vreau să văd vreun Rambo!”

În mod ironic, chiar şi atunci când un film prezintă în

mod fidel o scenă de luptă, cum se întâmplă de pildă în *Elicopter la pământ!* majoritatea criticilor îi reproşează că este nerealist. Totuşi, acesta este un film pe care instructorii de infanterie l-au recomandat tinerilor recruţi.

GENERAŢIA MTV

Războiul informaţional nu este dus numai împotriva inamicului, uneori trebuie să îl foloseşti şi pentru tine. În 2001, forţele armate americane s-au confruntat cu o situaţie de marketing dificilă. Ţinând cont de faptul că generaţia MTV nu este foarte impresionată de poveştile de glorie militară de pe vremuri, oficialităţile au dorit să vină în întâmpinarea tinerilor pe un teren cunoscut lor. Un nou show TV, numit *Wargames,* completat de o bandă sonoră, a fost văzut ca un mijloc excelent de promovare în rândul tinerilor recruţi. De asemenea, Marina a ajutat la realizarea unui reality show numit *Boot Camp,* în care participarea instructorilor încă în activitate a adus un plus de autenticitate. Au fost refăcute reclame de recrutare sub forma unor videoclipuri muzicale. Se punea accent pe acţiune şi entuziasm. În lunga istorie a recrutărilor militare, punerea accentului pe distracţie (care întotdeauna există) şi neglijarea oboselii, a stresului şi plictiselii a dat mereu rezultate mai bune decât spunerea adevărului despre cum este viaţa militară, întotdeauna a prins evidenţierea serviciului, a realizărilor şi a mândriei de a face ceva. Dar campania de atunci nu se referea atât de mult la recrutare, cât la aducerea la cunoştinţa oamenilor că forţele armate încă există. Recrutorii tind să fie mai direcţi în ceea ce priveşte viaţa adevărată de militar. Ei ştiu că zvonurile lansate de cei tineri aflaţi în serviciu sau de cei care au fost sunt folosite de posibilii recruţi pentru a furniza informaţii mai realiste despre cum este „în interior”. Dar majoritatea potenţialilor recruţi abia dacă ştiu că armata există. De aici şi invazia actuală de programe militare. Nimic nu părea să funcţioneze. Nici

măcar ardoarea patriotică stârnită de atacurile din 11 septembrie 2001 nu a mărit numărul recruţilor. Dar nici nu s-a micşorat.

VEŞTI DE DEPARTE

Înmulţirea posturilor TV a fost văzută iniţial ca un lucru bun. Mai multe opţiuni dădeau oamenilor posibilitatea să vadă ce doreau, nu numai ce era disponibil. Apariţia mai multor posturi de ştiri a fost de asemenea privită cu ochi buni. Mare parte din acest avânt s-a datorat reţelelor de ştiri disponibile la nivel mondial provenind din mai multe ţări. Acest lucru a permis imigranţilor din SUA să vadă ştiri într-o limbă pe care o cunoşteau. Dar războiul terorii început în 2001 a adus cu el un dezavantaj neprevăzut. Atacurile din 11 septembrie 2001 au fost dezbătute de staţiile de ştiri arabe într-un mod foarte diferit de cel din mass-media americană. Arabii au menţionat lucruri precum faptul că în spatele atacurilor de la World Trade Center s-a aflat Israelul sau că războiul împotriva terorismului este o scuză pentru războiul împotriva Islamului. Pentru mulţi arabi din America, acestea au fost singurele ştiri auzite. Acest lucru i-a pus într-o situaţie dificilă faţă de ceilalţi. Tindem să credem mare parte din ceea ce vedem la ştiri şi dacă două grupuri de oameni văd două interpretări diferite ale aceleiaşi poveşti, de ambele părţi vor exista suspiciuni şi situaţii stânjenitoare. Dar majoritatea celor prinşi în această situaţie şi-au extins lista de surse de ştiri, mai ales prin internet, înţelegând ceva mai multe despre cei care sunt diferiţi ca religie şi cultură. În acelaşi timp foarte mulţi oameni profită de noile posturi de ştiri străine disponibile pentru a căuta mai multe variante ale aceleiaşi informaţii. Nici nu trebuie să înţelegi alte limbi pentru a face acest lucru. Unele posturi străine transmit un grupaj al ştirilor în engleză, oferindu-le vorbitorilor de engleză un rezumat al evenimentelor zilei aşa cum sunt ele văzute în ţara lor.

Mulţi americani devin tot mai interesaţi, sau cel puţin consumatorii de ştiri, obţinând astfel o gamă mai largă de interpretări.

Chiar şi înainte ca reţelele de ştiri prin cablu să îşi extindă aria de acoperire în ultimii ani, internetul mergea pe această cale. Ziarele apăreau şi pe internet. Odată ce gazetele şi-au dat seama că nu vor pierde un număr mare de cititori dacă pun la dispoziţie variante online, a devenit obligatoriu să îşi facă simţită prezenţa şi pe internet. Acelaşi lucru l-au făcut şi marile ziare străine, dar nu numai pentru prestigiu. Naţiunile care aveau numeroşi imigranţi trăind în SUA au văzut în varianta online a ziarelor un mod de a păstra legătura cu cei din ţară. Varianta în engleză a ziarului pakistanez *Dawn* a devenit online în 1996. Redacţia ştia că mulţi dintre pakistanezii de peste ocean sunt oameni educaţi care îşi pot permite să fie pe net. Mai mult, pakistanezii care îşi făceau studiile peste ocean aveau acces la web de la universitate. Cei mai puţin înstăriţi foloseau internet cafeurile, fiind o metodă ieftină de a comunica cu familia de acasă. Ediţia online a ziarului *Dawn* a devenit din ce în ce mai populară. Oamenii din toată lumea care erau interesaţi de afacerile din Asia de Sud au dat peste acest ziar, care, deşi relata ştirile din punctul de vedere al pakistanezilor, era destul de imparţial.

Dar ziarele de pe internet nu au contracarat totuşi propaganda şi lucrurile neverificate care treceau de obicei drept ştiri pe alte site-uri şi mai ales la unele posturi de ştiri. Războiul împotriva terorismului a scos la iveală o mulţime de ţicniţi şi bârfitori care şi-au găsit pe internet un public avid de informaţii. Şi politicienii puteau intra în joc cu unele dintre cele mai interesante canale de ştiri. Un caz special a fost Al Jazeera, un post de ştiri în arabă difuzat în Qatar şi finanţat de emirul Qatarului (care este şi conducătorul federal al ţării). Deşi se spune că este una dintre puţinele voci libere ale jurnalismului din lumea

arabă, Al Jazeera este numai în mod aparent o agenţie de ştiri independentă. Cu toate că emirul este un om destul de blând şi nu conduce Qatarul cu autoritate, Al Jazeera tinde să trateze cu îngăduinţă ţările (şi politicienii) prietene cu emirul. Are noimă. Dar întotdeauna este sezon de vânătoare pentru cei din Vest şi în special pentru SUA. Ceea ce îi conferă acestui post mai multă credibilitate decât merită este maniera profesionistă în care prezintă ştirile. Din moment ce este în arabă, cei care nu vorbesc această limbă nu pot interpreta singuri conţinutul.

Este mult mai ieftin să pui la punct un site profesionist care să relateze despre toate ştirile. Dar nu vei atrage nici pe departe la fel de multe priviri ca atunci când ai şi un post TV de ştiri. Mai ales unul care are finanţarea necesară pentru a transmite prin satelit. Internetul este minunat pentru a da naştere poveştilor (adevărate sau false) şi pentru a răspândi idei prosteşti. Dar dacă vrei să te extinzi şi să ai o acoperire serioasă, trebuie să cheltuieşti bani.

Oricât de mult succes a avut Al Jazeera în timpul Războiului din Afganistan, declarând că această ţară nu va fi cucerită şi că lumea arabă se ridica pentru a-i apăra pe afganii nevinovaţi, în scurt timp credibilitatea postului a început să se clatine. Deşi acest lucru nu era surprinzător pentru lumea nevorbitoare de arabă, mulţi au fost şocaţi să vadă cât de repede greşelile postului au fost sesizate chiar de vorbitori de arabă. În mare parte, acest lucru se întâmpla pe internet, mai ales pe forumurile în engleză, dar şi pe site-urile tot mai numeroase în arabă.

O parte din contraatacurile asupra Al Jazeera erau conduse probabil de cyber-războinici profesionişti. Astfel de lucruri dau cele mai bune rezultate atunci când operatorii stau în umbră şi nu dezvăluie faptul că lucrează pentru guvernul american. Eficienţa unei astfel de abordări de gherilă a ştirilor se vede în faptul că departamentele de marketing din companii o folosesc de

ani de zile. Tehnica se numeşte „marketing viral”. Mai simplu spus, „agitarea apelor pe net”. „Agitarea” poate fi pozitivă sau negativă şi poate fi dirijată către o anumită ţintă. Cu alte cuvinte, am asistat la naşterea unei noi arme de cyber-război.

RECLAMA COSTĂ

Preluând o tehnică folosită des în politica americană, guvernul SUA a difuzat spoturi publicitare la posturile de televiziune arabe la sfârşitul anului 2001, expunând poziţia americană faţă de războiul împotriva terorismului cu toată strălucirea şi energia care fac filmele şi televiziunile americane atât de populare în ţările arabe. Al Jazeera este un post comercial şi, deşi se descurcă mai bine datorită reportajelor despre război, încă nu a devenit profitabil şi este considerat de tot mai mulţi oameni ca fiind antiamerican. Guvernul american a cerut ajutorul şi celor din industria de film, care îi include pe cei care creează reclamele. Mulţi regizori de film au început prin a regiza reclame şi clipuri video. Deşi nu au fost publicate niciun fel de reclame pe web, au fost puse în circulaţie multe materiale care explică poziţia oficială a Americii.

SE ÎNTOARCE ROATA

Războiul informaţional din Afganistan a fost dus cu aceeaşi sârguinţă cu care a fost dus cel cu bombe, dar se pare cu mai multă dibăcie şi inteligenţă. Pentru prima dată, internetul a fost o scenă de luptă majoră, cu trupe (atât voluntari, cât şi angajaţi) ce munceau pentru a oferi internetului supremaţie în lupta pentru influenţarea opiniei publice la nivel global. Pentagonul a recunoscut pentru prima dată importanţa bătăliei în mass-media şi a decis să ia măsuri în această privinţă în anii ’80. An după an, tot mai multe organizaţii guvernamentale au început să elaboreze strategii mass-media pentru viitoarele războaie. De data asta, această manipulare loveşte din plin, cu toate că americanii nu prea îşi dau seama de asta. De exemplu, mesajul care este ţintit către ţările musulmane se

concentrează pe asemenea lucruri; Saddam Hussein a ucis mai mulţi musulmani decât oricine altcineva în ultimul secol. Majoritatea războaielor împotriva musulmanilor din ultimii 50 de ani au fost purtate tot de musulmani. În ultimii zece ani, America şi-a trimis soldaţii de patru ori pentru a-i apăra pe civilii nevinovaţi (în Kuweit, Bosnia, Kosovo, Somalia). America a fost principalul lor susţinător în războiul împotriva ruşilor din anii ’80 şi a plătit pentru cea mai mare parte a ajutoarelor umanitare distribuite începând de atunci.

Pentru o vreme, America a fost văzută de mulţi dintre aliaţii noştri (mai ales europeni) ca pierzând războiul de propagandă. Înainte de a fi înfrânţi, talibanii făceau publice rapoarte despre numărul foarte mare de victime civile. Evident că multe dintre aceste declaraţii erau false. Dar prezentate unei audienţe imparţiale sau receptive, acele rapoarte pompoase au avut un efect negativ. SUA a răspuns prin creşterea eforturilor de a prezenta o versiune mai obiectivă a acestor rapoarte. O parte din acest efort a fost nimicirea, pe cât se poate, a informaţiilor înşelătoare care circulau pe internet. Aceste eforturi au dat roade şi rapoartele false sau distorsionate au dispărut. Simpla indicare a surselor vagi sau eronate a multora dintre aceste rapoarte a fost de ajuns. Dat fiind că talibanii plecaseră din Afganistan, a fost simplu de realizat acest lucru. Dar fără utilizarea internetului pentru a menţine în permanenţă în atenţia publicului subiectul (adevăratul număr al victimelor civile), majoritatea oamenilor încă ar mai crede că au fost ucişi 20.000 de civili (aşa cum susţineau talibanii), în vreme ce de fapt au fost sub o mie (fapt care a reieşit din intervievarea civililor din zonele bombardate).

În America trăiesc milioane (mai exact opt) de musulmani şi cel puţin 4.000 dintre aceştia slujesc în cadrul forţelor armate. Americanii care vorbesc arabă sunt folosiţi pentru a transmite prin intermediul posturilor TV şi

de radio în arabă mesajul autorităţilor. Deşi CIA a fost criticată pentru că s-a îndepărtat de „oamenii din teren” (agenţii din străinătate) în ultimii 20 de ani, acest lucru a fost făcut la insistenţele Congresului. În anii ’90, CIA a recrutat numeroase persoane pentru această activitate periculoasă şi vitală. În mod special, CIA a fost interesată de recruţii care cunoşteau limbi orientale. Armata a menţinut vreme îndelungată una dintre cele mai bune şcoli de limbi străine din lume şi a instruit lingvişti pentru unităţile sale secrete şi cele ale forţelor speciale. Internetul s-a dovedit a fi un instrument util pentru recrutări suplimentare. Nu numai că paginile web cu anunţuri de recrutare erau disponibile tot timpul, dar ele puteau fi rapid actualizate dacă ar fi existat vreun zvon despre subminarea eforturilor de angajare a unor cunoscători de limbă arabă. Cei mai potriviţi recruţi erau cei imigraţi recent, care în vreme ce au învăţat engleza nu au intrat în contact cu multe persoane în afara tovarăşilor imigranţi. Astfel de candidaţi pentru slujba de traducător este posibil să nu fi fost niciodată vizaţi de eforturile de recrutare ale guvernului.

Asemenea probleme lumeşti precum recrutarea traducătorilor pentru CIA ŞI FBI arată ce instrument uşor adaptabil este webul. Nu mă refer numai la recrutarea în sine, ci şi la abilitatea de a înfrunta în acelaşi timp grupările pro teroriste, de a descuraja procesul de angajare şi de a calomnia CIA ŞI FBI. Roata se învârte departe de privirea multora.

GOANA DUPĂ TITLURI PE PRIMA PAGINĂ

Războiul din Afganistan i-a deranjat pe mulţi jurnalişti, pentru că nu li se permitea accesul liber la operaţiunile militare americane. Unii dintre reporterii mai în vârstă îşi amintesc de perioada Războiului din Vietnam când puteau filma din mijlocul soldaţilor. Acest lucru nu se datora unei schimbări în politica guvernamentală; în

Vietnam nu a fost practic un război (ci doar un efort de asistenţă militară pentru Vietnamul de Sud). Oricine putea cumpăra un bilet de avion spre Vietnamul de Sud. Din cauza libertăţii de care jurnaliştii s-au bucurat în Vietnam, în timpul Războiului din Golf aceştia au fost foarte supăraţi din pricina restricţiilor care le-au fost impuse. Ceea ce îşi amintesc puţini dintre ei este că, în timpul războaielor purtate de America în ultimele secole, restricţiile erau norma. Forţele armate, chiar şi în Vietnam, îi suspectau pe jurnalişti că ar putea furniza informaţii preţioase inamicului. Acest lucru s-a petrecut pentru prima oară în 1860, în timpul Războiului Civil american. Armata, care fusese de multe ori măcinată în timpul Războiului hispano-american (din 1898, urmat apoi de răscoala din Filipine) şi în Primul Război Mondial (19171918), a dezvoltat un sistem agreat şi de ziarişti pentru cel de-al Doilea Război Mondial. Reporterilor de război li s-au dat uniforme, cu toate că nu erau consideraţi ca făcând parte din armată. În plus, ziarele şi posturile de radio pentru care lucrau continuau să îi plătească. Totuşi, reporterii de război erau hrăniţi şi adăpostiţi ca şi cum ar fi fost ofiţeri şi se supuneau legilor militare. Erau însoţiţi de ofiţeri de presă, iar relatările lor treceau pe la cenzorii militari înainte de a fi trimise acasă. Acest lucru trebuia făcut pentru a nu exista scurgeri de informaţii care ar fi putut provoca pagube. Dar astfel de incidente au avut loc în cazul unor operaţiuni de amploare precum Ziua Z şi spargerea codurilor japoneze de comunicaţie care a fost făcută publică în ziarele americane. Din fericire, naziştii şi japonezii nu aveau un acces rapid la acele articole din ziar, iar pagubele au fost diminuate. Dar acele incidente i-au speriat pe generali şi pe bună dreptate. În timpul Războiului din Vietnam, comuniştii au obţinut în mod constant informaţii utile despre operaţiunile americane prin monitorizarea presei din SUA. Restricţiile dure din timpul Războiului din Golf şi operaţiunilor din Afganistan

au fost determinate de problemele întâmpinate în Vietnam.

În timpul Războiului din Coreea, reporterilor li s-a cerut să apeleze la autocenzură. Dar nu întotdeauna a funcţionat şi mulţi jurnalişti au cerut ajutorul cenzorilor militari pentru a avea grijă ca nu cumva să se publice informaţii care ar putea afecta trupele. Deşi mulţi jurnalişti nu cunosc această parte a istoriei, ea este cunoscută de cei mai mulţi comandanţi militari cu experienţă. Acum, datorită expansiunii mass-media (mai ales a internetului) informaţiile vitale sunt mai uşor de obţinut şi de publicat de către inamic. Jurnaliştii îşi pot difuza ştirile în timp real, aşa că orice scăpare a departamentului informaţional îi oferă duşmanului un avantaj imediat. Nu e de mirare că armata este atât de dură cu jurnaliştii. Dar cum mulţi dintre aceştia nu înţeleg implicaţiile pagubelor pe care le pot provoca, pericolul este constant şi real.

RĂZBOIUL ZVONURILOR

Războiul împotriva terorismului a dat naştere şi la primele studii serioase despre cum sunt răspândite zvonurile pe internet. Bârfa tradiţională se răspândeşte încet, pentru că fiecare zvon este colportat pe rând, de câte o persoană. Dar pe internet zvonurile pot ajunge la mii sau chiar milioane de oameni în câteva zile şi pot fi eronate. Depinde de cât de suculentă, credibilă şi extraordinară este acea informaţie. De ani de zile, armata şi poliţia au delegat oameni care să monitorizeze paginile de ştiri, de chat şi *listserver-ele.* Aceşti agenţi „de ocazie” se pare că sunt organizaţi pentru a răspândi informaţii favorabile (militând pentru operaţiunile de antiterorism) sau pentru a dezinforma (informaţii false care vor răni, intimida şi distruge grupările pro-teroriste). Informaţiile de pe internet au câteva avantaje faţă de operaţiunile obişnuite de informare verbală. În primul rând, materialul este scris. Oamenii încă mai au un respect mai mare pentru datele scrise decât pentru ceea ce aud de la cineva.

De aceea sunt luate de bune atâtea ştiri îngrozitoare care apar pe net, dar care par relativ prosteşti atunci când sunt repetate verbal. Printre numeroasele zvonuri false lansate recent se număra şi acela că personalul multor companii arabo-americane (mai ales restaurantele) se înveselea atunci când apărea la televizor imaginea clădirii World Trade Center arzând. La o investigare mai atentă, nimic din toate acestea nu s-a dovedit a fi adevărat. Dar oamenii au crezut, nu pentru că le-a spus un vecin ceva, ci pentru că au „văzut informaţia pe internet". Dacă cineva le-ar fi spus-o faţă în faţă, numai punând câteva întrebări şi-ar fi dat seama că este doar un zvon.

Un alt avantaj este că pe internet îţi poţi crea mai multă credibilitate prin transmiterea câtorva informaţii ce pot fi probate înainte de a avansa informaţii false. Un operator priceput poate provoca multe pagube cu această tehnică. Cel mai bun exemplu este o strategie de tipul

„Umflă preţul şi scapă de acţiuni" despre care auzi la buletinele de ştiri despre investiţii. Este vorba despre un vechi truc pe piaţa de schimb în care cumperi acţiuni ieftine de la o companie slab dezvoltată şi apoi, pe internet, susţii că sunt nişte acţiuni subapreciate. Discuţia merge mai departe la cât de mult vor creşte acestea. Cei care câştigă un astfel de joc au un soi de lipici la public şi în unele cazuri au furnizat chiar unele informaţii bune. Dacă faci totul cum trebuie, victimele se vor îngrămădi să cumpere acţiunile pe care le-ai „umflat". Preţul urca vertiginos, moment în care tu „scapi" (vinzi) de acţiuni şi te alegi cu un profit bun.

Unul dintre instrumentele preferate în războiul antiterorist a fost folosirea informaţiilor false. Direcţionate spre ţinta potrivită, acestea ar putea avea un impact militar semnificativ. De exemplu, la scurt timp după 11 septembrie, au început să apară zvonuri că 4.000 de israelieni care lucrau la World Trade Center nu s-au prezentat la muncă pe 11 septembrie şi că atacul a fost

aranjat de serviciul secret israelian Mossad. Deşi pentru occidentali această teorie pare absurdă, sondajele de opinie din Pakistan de la începutul războiului indicau disponibilitatea populaţiei de a crede asemenea supoziţii; mai mult de jumătate dintre pakistanezi cred că atacul a fost opera israelienilor. Astfel de zvonuri au avut valoare militară în Războiul din Afganistan, întrucât SUA aveau nevoie de baze în Pakistan pentru a susţine operaţiunile din Afganistan, unde nu se putea pătrunde. Fundamentaliştii islamici au luat în serios zvonul despre Mossad şi lucrurile au fost neclare o vreme în timpul revoltelor şi demonstraţiilor pe care aceştia le-au generat. De asemenea, este important să ne amintim că webul are dimensiuni globale. În ţările arabe şi musulmane există milioane de indivizi cu acces la internet, iar în ţările mai sărace, internet cafe-urile sunt mai obişnuite. Aşa că nu este nevoie să ai un computer pentru a avea acces la web. Nu ai nevoie decât de suficienţi bani pentru a cumpăra o oră sau două de acces în fiecare săptămână sau lună pentru a ţine pasul cu ultimele zvonuri de pe internet. Afganistanul este una dintre puţinele ţări din lume fără acces uşor la web (trebuie să foloseşti un telefon prin satelit sau să treci graniţa către Iran sau Pakistan).

O altă poveste răspândită de autorităţile israeliene a fost ca atacul de la 11 septembrie părea să poarte inconfundabila semnătură a veteranului terorist al Hezbollah, Imad Mughniyah. Nu exista nicio dovadă concretă în acest sens, dar Israelul dorea să fie limpede că grupările teroriste Hezbollah şi palestiniene au legătură cu bin Laden (de fapt, relaţii existau, dar numai ocazional). Acest zvon a avut cel mai mare impact în Israel, unde s-a alăturat sentimentelor de ură deja existente la adresa Hezbollah şi israeliţilor. Cu atât de multe reţele de radio şi televiziune, consumatorii au auzit cele mai îngrozitoare zvonuri şi, ca într-un război informaţional adevărat, mulţi operatori au publicat variante care să le susţină cauza.

Totuşi, ceea ce ştiau mulţi războinici informaţionali era că modalitatea cea mai uşoară de a face ca o ştire să ajungă în mass-media era infiltrarea ei în câteva puncte strategice de pe web. Astfel stârneşti vâlvă şi în cele din urmă mass-media (scrisă sau electronică) va prelua ştirea. Au existat multe zvonuri lansate pe internet care susţineau teoria

„Mossadul a doborât turnurile" şi care au ajutat la păstrarea ei chiar şi după ce au apărut clipurile cu bin Laden care îşi revendica reuşita. Acele clipuri au generat o mulţime de discuţii pe net, inclusiv câteva descrieri despre cum le-ar fi putut falsifica Hollywoodul. Una dintre dezinformările de pe internet, care se află printre preferatele mele, este cea care susţine că filmuleţul în care Osama bin Laden discuta la cină despre atacurile din 11 septembrie era, de fapt, preluat dintr-un film mai vechi, în care el se afla la nunta fiului său în Afganistan. Zvonul a fost repede dezminţit prin compararea celor două filme, dar pagubele fuseseră deja făcute.

PĂSTRAREA PĂCII VIRTUALE

Din punct de vedere politic, a devenit periculos pentru americani să trimită militari în punctele fierbinţi de pe glob. Un astfel de punct este Israelul. Neliniştile de acolo sunt văzute ca o oportunitate pentru un război informaţional de cele mai multe canale mass-media, jucători politici şi diplomatici. Israelul este de multă vreme aliat al americanilor, iar ofiţerii SUA merg acolo în mod regulat pentru întâlniri, cercetări şi instruiri. Atunci când lucrurile se precipită, militarilor americani care urmau să viziteze Israelul li se comunică să reprogrameze venirea sau să fie înlocuiţi de civili în cazul în care anumite întâlniri nu pot fi contramandate.

De fiecare dată când se preconizează vreo violenţă politică (fie că este vorba de rebeli sau de terorişti) în ţări străine, presa caută trupele americane. Dacă sunt identificaţi militari şi chiar dacă ei nu fac nimic legat de operaţiuni militare (precum rezervarea unor clădiri pentru

instructajele anuale sau o echipă medicală ce oferă ajutor victimelor unui dezastru recent), cineva începe să facă legături. „Trupele SUA sunt în zonă”, spun titlurile de primă pagină, iar cititorii sunt lăsaţi să dea frâu liber imaginaţiei. O mare parte dintre acestea nu sunt tocmai parte dintr-un război informaţional în sens militar. Este doar generare de titluri pentru ziare care vor atrage mai multe priviri şi vor creşte veniturile din publicitate. Nu toată lumea ştie asta, iar poveştile nefondate au viaţa lor. De aceea, un general prudent îşi ţine trupele departe de zonele fierbinţi, pentru a evita apariţia unor efecte secundare nedorite şi nejustificate.

Internetul a venit cu o soluţie pentru această problemă, care, la rândul ei, a mai adăugat o armă la arsenalul modern al soldaţilor. În ultimii 20 de ani (din ultima perioadă a ARPANET-ului), armata a devenit interesată de aşa-zisul „studiu la distanţă”. E vorba de mai mult decât simplul control al corespondenţei de pe internet. Abordarea militară include folosirea unor simulări de luptă realiste (wargames pentru civili) şi generarea unui număr mare de e-mailuri înainte (pentru planificarea exerciţiului) şi după (pentru discutarea concluziilor) cu privire la jocul în sine. Nu toate trupele călătoresc peste ocean pentru a se angaja într-o luptă, nu puţini sunt cei care pleacă pentru a vedea ce şi cum fac aliaţii sau posibilii aliaţi. Se pare că e-mailul însoţit de imagini digitale şi filme poate înlocui documentare la faţa locului făcând inutilă o călătorie.

Un plus al acestei strategii este acela că este asigurată armonia conjugală pentru soldaţii căsătoriţi, care pot înlocui călătoriile cu internetul, astfel departe de familiile lor mai rar şi pentru mai puţin timp. Iniţial, singurele naţiuni cu care puteai face asta erau cele industrializate (cu un bun acces la internet şi cu mulţi utilizatori de net). Atunci când World Wide Webul a apărut pe scenă, a devenit tot mai evident pentru trupele

americane că armata chiar şi din cele mai sărace ţări avea cele mai multe şanse de a găsi o mulţime de utilizatori de internet. În cele mai sărace ţări, armata este, fără a pune la socoteală universităţile, cea mai tehnologizată organizaţie.

Ideea de „luptă la distanţă” a luat naştere în armata americană la sfârşitul anilor ’70. Dat fiind modul în care îşi făceau proiectele loc în armată, de abia în anii ’80 au ajuns la trupe aceste reţele de instructaj. Când a fost lansat World Wide Webul, oamenii din armată (nu numai americanii) au realizat că tehnologia de care aveau nevoie se dezvolta mult mai repede (şi mai ieftin) în sectorul comercial. Armata cumpărase tehnologii de la companiile care creaseră jocurile pentru reţea şi îşi instruise militarii cu ele. Acest lucru are o foarte mare semnificaţie militară pentru că, până să apară internetul, SUA deţinuseră supremaţia în ceea ce priveşte instructajul cu înaltă tehnologie. Sistemele de instruire dinaintea internetului erau scumpe şi numai SUA şi alte ţări înstărite şi le puteau permite. Dar acum şi cele mai sărace ţări pot cumpăra simulări de război realiste şi pline de efecte vizuale pe care le pot folosi pentru instruirea propriilor militari. Până şi ţările sărace îşi dau seama că furnizarea accesului la internet are un mare efect moralizator pentru trupe.

VIITORUL RĂZBOIULUI INFORMAŢIONAL

Cât de bine va funcţiona războiul informaţional în viitor? Uite ce s-a întâmplat în timpul Războiului din Golf din 1991. Coaliţia (naţiunile ce luptau în Irak) avea cea mai mare parte a armelor informaţionale, dar Irakul nu era uşor de învins. Având acces la mass-media mondială, Irakul a încercat, cu un oarecare succes, să convingă opinia publică să îi susţină cauza. De fapt, cauza Irakului a rămas populară în opinia generală din multe ţări arabe sau din lumea a treia. Credinţa irakienilor era că ei deţineau Kuweitul şi că tot ei apărau onoarea arabă prin înfruntarea occidentalilor care încercau să îi scoată din Kuweit. Din

cauza modului în care conducerea irakiană a prezentat situaţia la CNN şi la alte posturi internaţionale, „ofensiva mass-media” a acestei ţări a avut un impact şi asupra opiniei publice din naţiunile cu care se luptau. Agenţii irakieni din afara Irakului au încercat să saboteze reţelele militare din ţările coaliţiei.

Şi alte naţiuni care ar putea merge la război au învăţat lecţiile Irakului şi ale războiului informaţional. În războaiele viitoare cel mai slab va profita cel mai mult de un post precum CNN-ul.

Ştirile TV sunt întotdeauna în căutare de poveşti îngrozitoare care vor atrage privirea şi multe naţiuni îşi dau seama că există un avantaj militar ce poate fi câştigat dacă intri în acest joc. Am avut de multe ori parte de aşa ceva de la Războiul din Golful Persic încoace. În Războiul din Afganistan, talibanii au lucrat după modelul irakian. Tot atunci a ieşit le iveală un alt element-cheie: timpul. Războiul s-a terminat înainte ca eforturile talibanilor să ducă la vreun rezultat.

De asemenea, a mai avut loc un război informaţional în timpul Războiului din Golf din 1991 sau cel puţin se pregătea pentru unul. Acesta era cel care putea amenința milioanele de mesaje care au circulat între unităţile Coaliţiei din Arabia Saudită şi acele unităţi şi organizaţii care le susţineau de acasă. Irakienii nu au fost în stare să producă prea multe pagube în acest sector, dar cel puţin au încercat. Cele mai eficiente pentru ei erau acele tehnici de război informaţional greu de depistat în timp util. De exemplu, să luăm situaţia în care duşmanul putea şterge o parte din mesajele tale. Ţi-ar fi luat ceva vreme până să îţi dai seama de ce se întâmplă şi mai multă să rezolvi confuzia rezultată. Pagubele ar fi majore. Piesele de schimb ar fi trimise lăsând echipamentul nefolosit. Unităţile nu ar mai primi ordinele de deplasare sau ordine de schimbare a locaţiei.

Problema aceasta, a duşmanului care putea intra în

reţeaua ta de comunicaţii, de unde putea şterge mesaje, a devenit un subiect fierbinte la începutul anilor ’90 când s-a observat cât de vulnerabile sunt liniile de comunicaţie ale lumii în faţa acestui tip de atac. Se presupune că lucrurile ar trebui să se fi rezolvat sau pe cale să se rezolve. Dar cine poate fi sigur?

În urma Războiului din Golf a mai apărut o problemă posibilă. S-a observat că unităţile aeriene, terestre şi navale devin mult mai dependente de propria reţea locală de computere. Flota a descoperit că este deosebit de vulnerabilă întrucât în cazul unei misiuni navale urgente, nu ar putea aduce experţi în tehnologie în apropiere sau resurse pentru a putea face faţă unui atac asupra reţelelor. Nu numai că fiecare navă are mai multe „plase”, dar toate cele vreo şase dacă nu mai multe nave implicate sunt conectate la o reţea şi mai mare, astfel încât toate sistemele de apărare şi de atac ale navelor să poată fi unite împotriva duşmanului. Când flota americană a analizat mai cu atenţie structura reţelei, a descoperit că este destul de vulnerabilă. Nu ai auzit prea multe despre acest lucru, pentru că nimeni nu ştie cine se ocupă de problemă. Reţelele militare americane erau mult mai robuste în Războiul din Afganistan. Din fericire, inamicul nu a fost prea bine echipat pentru a le ataca.

În 1999, NATO a declarat război Serbiei, iar sârbii, în lipsă de arme, au apelat la războiul informaţional. De fapt, sârbii au forţat adeseori NATO să pună la bătaie cele mai avansate tehnologii. Dar sorţii n-au fost de partea lor şi în cele din urmă NATO a câştigat. Serbia a făcut câteva încercări slabe de a ataca pe internet, dar nu a avut succes. Au avut succes cu modificarea sistemului aerian de apărare, astfel încât au ajuns să poată doborî avioanele secrete ale SUA (pentru prima dată).

În timpul Războiului din Afganistan din 2001, duşmanul a avut chiar şi mai puţin succes cu războiul informaţional. Talibanii şi al-Qaeda şi-au jucat bine şansele

şi nu s-a petrecut nimic până nu a devenit evident că cei mai mulţi afgani sunt bucuroşi să scape şi de talibani, şi de al-Qaeda.

Irakul încă mai duce un război informaţional pentru a scăpa de sub sancţiunile Naţiunilor Unite. Este puţin probabil să câştige, dar din cauza modului bine pus la punct în care Irakul a acţionat până acum, încă nu pot fi înlăturaţi prea uşor.

Forţele armate americane în mod special şi cele ale altor naţiuni industrializate sunt tot mai dependente de comunicaţiile electronice şi tot mai vulnerabile la atacurile informaţionale. Armele superioare folosite de trupele americane funcţionează atât de bine pentru că răspândesc cu viteză datele pe câmpul de luptă. Dacă întrerupi acest curs al comunicării, vei distruge supremaţia înaltei tehnologii. Este dificil să selectezi informaţiile, dar nu imposibil pentru o naţiune cu ingineri şi cercetători bine pregătiţi în Occident. Staţiile de bruiaj şi receptoarele de examinare a semnalelor folosite de americani pot, în mâinile unor oameni care-şi cunosc interesul şi sunt bine pregătiţi tehnic, să anihileze armele minune moderne. Bombele îşi vor rata ţintele într-un procent mai mare, comunicaţiile vor fi întrerupte sau interceptate şi băieţii răi vor fi mult mai greu de învins. Numărul victimelor va fi mai mare şi băieţii buni vor fi mai puţin încrezători în armele şi echipamentele lor.

Ultima parte nu este un lucru chiar atât de rău, dar astfel de dezastre sunt greu de prevăzut pe timp de pace. Este dificil să recreezi sentimentul de teamă al unui inamic ce dispune de o tehnologie mai puţin avansată şi care urmează să fie lovit de o armată cu tehnologie de ultimă generaţie. Autoconservarea este un foarte puternic stimulent şi multe naţiuni nedezvoltate tehnic au fost foarte motivate de rezultatele Războiului din Golf.

Ar putea exista deja un exemplu în acest sens. În 2001, bombele inteligente americane ghidate prin GPS au

ratat toate ţintele irakiene de la aceeaşi distanţă şi în aceeaşi direcţie. Experţii americani în arme spun că este vorba despre o eroare de programare din partea tehnicienilor. De asemenea, există posibilitatea ca irakienii să fi folosit staţii de bruiaj prin GPS. Semnalul GPS (de la sateliţi spaţiali) este slab şi uşor de bruiat. Timp de mai mulţi ani, producătorii de bombe inteligente au lucrat la crearea unor sisteme care să nu poată fi bruiate, dar armele cu această funcţie nu au fost puse încă în practică. Mai multe naţiuni se laudă că vând staţii GPS de bruiaj, printre care şi Rusia. Tehnologia de bază a acestui dispozitiv este îndeajuns de simplă pentru ca irakienii să îşi facă una proprie. Chiar dacă nu sunt sprijiniţi de nimeni. Este interesant de notat că bombele inteligente americane prin GPS au un sistem de ghidare de rezervă, mai puţin precis (dar care nu poate fi bruiat) în cazul în care sistemul GPS este distrus, dar această rezervă nu intră în funcţiune dacă semnalul GPS este doar uşor bruiat. Ne-au bruiat irakienii bombele inteligente cu ajutorul GPS-ului? Această „problemă” cu bombele a avut loc o singură dată. Poate că irakienii pur şi simplu îşi testau aparatura să vadă dacă funcţionează. Un sistem de bruiere GPS cu adevărat performant nu ar pune în funcţiune sistemul de ghidare de rezervă. Dacă irakienii au creat (ori au cumpărat) un asemenea sistem, îl vor păstra pentru a-l folosi în cazul unui atac major al SUA. Dacă irakienii nu au acest sistem, cineva cu siguranţă îl are sau îl va avea. Şi piloţii americani vor trebui, în cele din urmă, să îi facă faţă.

Piloţii şi luptătorii de la sol americani sunt conştienţi de cât de relativ este avantajul înaltei tehnologii. Toate dispozitivele noi sunt privite cu scepticism de către trupele de luptă, mai ales de când noua tehnologie le este oferită cu ordinul de a „o folosi”. Trupele adoptă o atitudine de genul

„Dacă nu-mi iese nimic, e inutilă”. Cu alte cuvinte,

câmpul de luptă este înţesat de noi echipamente în care trupele nu au încredere. Totuşi, ele nu sunt folosite decât după ce mai mulţi militari mor în luptă. Războiul informaţional aduce în prim-plan un alt tip de soldat de linia întâi, operatorul de echipament sau expertul în tehnologie. Desigur, echipajele de pe tancuri şi mulţi infanterişti folosesc deja un număr de dispozitive de înaltă tehnologie (iluminatoare de ţintă cu laser, diferite tipuri de radiouri, bombe portabile, senzori), dar multe dintre acestea au nevoie de specialişti care să le dirijeze foarte aproape de front. Aparatura de război electronică este tot mai mică şi mai uşor portabilă. Tot mai mult echipament este scos în faţă şi tot mai mulţi oameni care credeau că vor fi doar „tehnicieni" se trezesc de multe ori în bătaia focului. Pe lângă informarea cât mai corectă a operatorilor cu privire la viitoarele condiţii de muncă, există de asemenea tendinţa de a crea noi echipamente suficient de simple încât majoritatea specialiştilor militari tradiţionali (infanterie, echipajele de pe tancuri) să le poată manevra.

CAPITOLUL 7
HACKER, SYSADMIN ŞI CODE WARRIOR
TERMENI TEHNICI

Glosarul complet, ce include şi termenii definiţi mai jos, poate fi găsit la sfârşitul cărţii.

Poliţia cibernetică – oameni ai legii (plus un număr de profesionişti ai internetului care îşi oferă ajutorul voluntar) care iau urma infractorilor ce operează pe internet. În anii '90, cei mai mulţi dintre aceştia învăţaseră tainele meseriei pe cont propriu (poliţişti pentru care computerul era un hobby), dar acum există un mare avânt de a-i instrui pe mulţi dintre oamenii legii astfel încât să poată face faţă infracţiunilor pe internet.

Magnetul minţilor sclipitoare – orice organizaţie sau activitate care atrage mulţi oameni cu bune abilităţi de operare pe computer şi internet. Corporaţia Microsoft este un astfel de magnet, la fel cum sunt şi unele tipuri de software (precum sistemele de operare Linux).

OPSEC – termenul militar pentru operaţiunile de securitate. Aceasta este denumirea pentru acţiunile pe care le întreprinzi pentru a împiedica duşmanul să intre în serverele bazelor, clădirilor sau de internet.

Script Kiddies sunt în general tineri, de multe ori adolescenţi care-şi fac de cap pe internet prin utilizarea instrumentelor de hacking uşor disponibile. Aceştia sunt mai mult o pacoste decât o ameninţare, dar plecând de aici, unii trec la hacking serios, ajungând la infracţiuni.

Aceştia sunt oamenii datorită cărora există internetul său, în unele cazuri, nu există.

Hackerilor le place să creeze programe, mai ales dacă au legătură cu internetul. Administratorii de sistem sunt cei responsabili de întreţinerea a milioane de servere (care furnizează cele două miliarde pe pagini web pe care le accesăm cu toţii). Un code-warrior este cel care atacă sau apără software-ul internetului. Totul se rezumă la software, la miile de programe care ţin internetul în funcţiune. Noţiunile de hacker, sysadmin şi code-warrior se referă la oamenii care creează, repară, supraveghează sau încearcă să distrugă acest software.

CE ÎNSEAMNĂ HACKER, SYSADMIN ŞI CODE-WARRIOR?

Oamenii din prima linie a oricărui cyber-război sunt o specie aparte. Software-urile şi sistemele pe care funcţionează sunt create şi conduse de ingineri şi programatori, deloc departe de personajele comice din benzile desenate Dilbert. Asta pentru că programarea este în acelaşi timp artă şi ştiinţă, motiv pentru care programatorii tind să fie consumaţi de activitatea lor.

Afirmaţia potrivit căreia aceştia ar fi inapţi din punct de vedere social este de obicei exagerată, numai că programarea este genul de muncă pe care o faci şi acasă.

Cyber-războiul înseamnă mai mult decât programare; mai sunt şi administratorii de sistem.

Slujba lor a evoluat odată cu computerele conectate. La început (în anii ’60), reţelele de calculatoare erau atât de complexe, încât era nevoie de un inginer pentru a le păstra în funcţiune, în anii ’70, au început să apară LAN-urile (Local Area Networks) relativ uşor de folosit şi foarte populare (pentru că erau mai ieftine şi mai simplu de utilizat). În anii ’80, tehnologia reţelelor a ajuns atât de obişnuită, încât nu era ceva neobişnuit ca unui simplu angajat să îi fie aruncat un manual de utilizare şi să i se spună: „Tu eşti administratorul de sistem, nu o da în bară”. Evident, mulţi dintre aceştia nu prea ştiau ce fac. Sau atunci când ştiau, nu aveau timp pentru asta. Să fii administrator de sistem înseamnă, de multe ori, să ai o slujbă part-time. În cea mai mare parte a timpului, reţelele merg bine, dar atunci când se strică, se poate întâmpla ca administratorul cu jumătate de normă să nu poată rezolva problema. Acest fapt le-a dat mult de lucru consultanţilor, dar nu a rezolvat problema proastei administrări a sistemului. În principiu, asta însemna că software-ul LAN nu era actualizat corespunzător sau era modificat pentru a-i îmbunătăţi performanţele şi securitatea. Aceasta a fost veriga slabă a securităţii internetului timp de două decenii, iar lucrurile nu par să se îmbunătăţească.

Cei care lucrează la web sunt tehnicieni, persoane care oferă consultanţă, persoane de interfaţă care nu creează software, dar care se implică zilnic în susţinerea internetului. Ei sunt ochii şi urechile internetului, cei care văd prima dată când ceva merge prost. Dacă se va declanşa un cyber-război, ei sunt cei care îl vor simţi primii.

Termenul de code-warrior se referă la cele câteva mii

(majoritatea bărbaţi) de programatori de elită şi ingineri care ştiu o grămadă de lucruri (dar nu tot) despre ce se petrece înăuntrul celor câteva mii de programe care asigură buna funcţionare a internetului. Cei mai mulţi au lucrat la un astfel de software la un moment dat în carieră. Aici sunt incluse software-ul serverului web care rulează pe multe alte site-uri şi software-ul din rutere şi din site-urile de comunicare care sunt coloana vertebrală a internetului (liniile de fibră optică ce transmit cea mai mare parte din datele de pe internet pe distanţe mari).

În timpul anilor ’90, securitatea internetului şi a reţelelor a devenit o mare problemă. Deşi organizaţiile mari (ISP-uri precum AOL şi corporaţiile uriaşe) şi-au format propria reţea de operaţiuni de securitate, majoritatea computerelor conectate la internet nu erau actualizate în mod regulat cu software-ul de pe internet. Ca răspuns la această situaţie au apărut companiile care creau software de securitate comercial, la fel ca şi firmele de consultanţă care puneau la dispoziţie oameni pricepuţi în detectarea intruziunilor de orice fel. Internetul este o structură atât de complicată, încât există multe locuri unde ar putea fi vulnerabil în faţa unor răufăcători. Până acum, cea mai populară soluţie este să instalezi un software care urmăreşte intrările abuzive, pe care le opreşte sau alertează administratorii de sistem. Dar chiar şi pentru instalarea acestui software este nevoie de cineva care să ştie multe despre internet (cu alte cuvinte, un consultant scump).

Problema era şi încă mai este aceea că există prea multe părţi din software cu erori şi care sunt vulnerabile la atacuri. Administratorii de sistem caută cu disperare o soluţie pentru acest lucru. Domeniul securităţii reţelelor este atât de bine plătit şi furnizează o activitate atât de interesantă încât, de obicei, un code-warrior abil îşi părăseşte compania pentru a se alătura unei companii de software de securitate sau consultanţă.

Chiar şi armata are această problemă. În anii ’90, multe organizaţii din Departamentul Apărării au pregătit operaţiuni cyber-războinice.

Dar nici chiar bonusurile şi medaliile nu i-au făcut pe funcţionari să fie la fel de pregătiţi precum un expert în securitate din exterior.

În lumea securităţii internetului, există patru grupuri implicate:

Cel mai mare, ajungând la milioane de membri, este format din adolescenţi în căutare de senzaţii tari pe internet, care folosesc instrumente de hacking accesibile. Cei mai mulţi dintre ei scapă; foarte puţini sunt prinşi şi judecaţi. Câţiva îşi îmbunătăţesc abilităţile şi se alătură hackerilor black hat (tipii răi, dar pricepuţi).

— Administratorii de sistem. Şi ei ajung la numărul milioanelor, dar majoritatea dintre ei lucrează part-time şi mulţi se pricep foarte bine la computere. Administratorii de sistem sunt prima linie de apărare pe internet. Pentru operaţiunile de mare importanţă, aceştia sunt foarte bine instruiţi şi pregătiţi. De aceea organizaţii precum AOL, General Motors sau băncile mai importante funcţionează destul de bine, cu toate că sunt în permanenţă atacate de mii de amatori şi profesionişti. Reţelele mai mici au administratori mai puţin pregătiţi, iar cei mai mulţi dintre utilizatorii de modemuri prin cablu sau conexiuni DNS nu îşi dau seama că maşinăriile lor sunt la fel de vulnerabile ca o reţea fără administrator, fie el şi angajat cu jumătate de normă.

— Hackerii white hat. Sunt mai puţin de o sută de mii de persoane care aparţin acestui grup şi totuşi sunt cei care au pregătirea să-i urmărească pe hackerii mai periculoşi. Nimeni nu a făcut un calcul exact, părerile sunt împărţite, dar ei sunt experţii care pot înfrunta problemele serioase de pe internet. Armele de top sunt cu miile, dar numărul celor consideraţi la nivel mondial „code-warrior de top” se restrânge la câteva sute. Unii dintre ei sunt

consultanţi, alţii lucrează în alte părţi din industria software-ului sau a internetului. Reputaţia lor este recunoscută printre superiorii lor (profesioniştii software din industria internetului).

— Hackerii black hat. Mulţi lucrează pentru organizaţii criminale, dar au pregătirea unui code-warrior. Alţii sunt în mod oficial cyber-războinici pentru guvernele care pun la cale un cyber-război împotriva SUA (China în mod special). Numărul lor este de aproximativ 5.00010.000, în funcţie de cât de bine pregătit ar trebui să fie cineva pentru a provoca pagube majore.

Programatorii sunt cei care creează software-ul pe baza căruia funcţionează orice computer. De obicei, programatorii îşi găsesc repede de lucru şi parcă niciodată nu sunt suficient de mulţi programatori buni. În 1983, când PC-ul începea să devină popular, Biroul de Statistică a Muncii din SUA număra numai 278.000 de programatori. Zece ani mai târziu, atunci când World Wide Webul a devenit un fenomen cultural, existau 639.000 şi încă se mai căutau. În 2000, erau 1, 1 milioane de programatori şi erau încă la şi mai mare căutare. Estimările actuale spun că până în anul 2010 vor exista două milioane.

Din păcate, tot vor fi puţini, chiar şi dacă ar exista milioane de programatori din afara SUA dornici să imigreze. Motivul ar fi că programarea este o carieră dificilă. Este şi artă, şi ştiinţă, şi muncă grea. Cei mai mulţi dintre cei care devin programatori şi capătă destule abilităţi pentru a face o asemenea treabă părăsesc domeniul în mai puţin de zece ani. Angajatorii au descoperit că este mai bine să ai mai puţini (sau chiar un singur) programatori foarte buni decât să foloseşti inşi mediocri.

Din fericire, mulţi hackeri competenţi nu lucrează pe internet de dimineaţa până seara; singurii care fac asta sunt cei angajaţi de guvern pentru operaţiunile cyber-războinice. Atunci când văd că se petrece ceva interesant

pe web (o eroare de software sau apare nevoia unui alt instrument), se implică activ. Slujbele oferite de guvern sunt tot mai numeroase pe măsură ce ţările se pregătesc de cyber-război. Hackerii black sau white hat sunt o altă problemă. În anii ’90, Europa de Est era un paradis al hackerilor mercenari (care erau fie black hat, fie white hat, în funcţie de ce erau plătiţi să facă). Guvernele din Europa de Est erau distrase de problemele economice şi politice, iar unele dintre ele erau atât de corupte încât ofereau protecţie sau chiar angajau hackeri renegaţi şi rămaşi fără slujbe. Deşi crima e plătită, mai ales cyber-crima, nu este ceva obişnuit printre marile puteri economice ale lumii, fapt care a dus la crearea unei rupturi a acestor grupuri la începutul secolului

XXI. Guvernele şi companiile au creat organizaţii ale infracţiunilor pe computer care au transformat hackingul criminal într-o ocupaţie periculoasă. Chiar şi cu numărul tot mai mare al poliţiştilor cibernetici, spaţiul virtual va deveni din ce în ce mai periculos. Întotdeauna vor exista tentaţii pentru hackerii black hat de a câştiga un ban în plus.

Se bănuieşte că mare parte din pirateria de pe internet este făcută de neprofesionişti. Infracţiunile cibernetice se vor înmulţi, dar o parte dintre cyber-războinici se vor trezi că îşi folosesc abilităţile pentru operaţiunile guvernului dintr-un cyber-război. Rusia şi China au făcut cyber-criminalilor talentaţi pe care i-au capturat o ofertă de nerefuzat („Lucrează pentru noi sau ajungi la închisoare.”)

Dar există şi un număr foarte mare de hackeri white hat şi sunt mult mai mulţi decât cei din tabăra adversă. Celor mai mulţi oameni nu le place să fie atacaţi de un black hacker, iar mulţi dintre aceştia din urmă au fost prinşi pentru că white hackerii trec la soluţionarea cazului. Acest lucru a făcut ca multe organizaţii de poliţie (şi inşi din FBI) să cunoască hackeri white hat talentaţi. Pentru că

programatorii buni ştiu că sunt bine pregătiţi şi pentru că ei înşişi sunt pretenţioşi în privinţa locului în care vor lucra, de multe ori evită slujbele oferite de guvern sau armată. Pentru că hackerii white hat şi poliţia au în comun dorinţa de a-i prinde pe tipii răi, aceasta din urmă îi poate cel puţin chema pe consultanţii white hat, uneori în calitate de voluntari, pentru a rezolva cazurile de infracţionalitate cibernetică. Nu este vorba despre faptul că poliţia nu le poate plăti hackerilor white hat banii pe care aceştia deja îi câştigă. Dar acei white hackeri nu vor să îşi petreacă tot timpul prinzându-i pe tipii răi. Însă SUA beneficiază de un număr imens de hackeri bine intenţionaţi. În cazul unui război, tot acest talent se va dovedi a fi un veritabil bun militar naţional.

ASN NU ESTE UN MAGNET PENTRU MINŢI SCLIPITOARE

Una dintre marile probleme pe care le are de înfruntat ASN (Agenţia pentru Siguranţă Naţională) odată cu progresul tehnologiei internetului şi al criptării (codurile secrete) este propria neîncredere în a-i angaja pe mulţi tineri programatori. Acesta este rezultatul unei rupturi de generaţii şi cultură. La începuturile ASN, în anii ’50 şi 60, agenţia a angajat programatori pregătiţi în cultura tradiţională a computerelor obişnuite. Revoluţia PC-urilor a sărit peste ASN şi acum cei de aici se găsesc în situaţia de a fi destul de puţin echipaţi pentru a face faţă noilor tehnologii care s-au dezvoltat în ultimele două decenii. ASN s-a concentrat întotdeauna pe computerele făcute special (pentru crearea şi spargerea codurilor secrete). Pe măsură ce computerele cu devenit tot mai puternice, ASN a rămas în urmă, ratând dezvoltarea noilor instrumente şi tehnici software create pentru aceste calculatoare produse în masă. În anii ’90 se putea face criptarea pe PC şi asta mult mai ieftin şi cu mai puţin efort. De aceea tinerii programatori au văzut în ASN o structură de modă veche şi ostilă noilor idei. Tânăra generaţie de

programatori a avut reţineri în a se înscrie în programe de securitate naţională. Această dificultate în procesul de recrutare este des întâlnită în guvern, pentru că sectorul comercial oferă slujbe mult mai atrăgătoare (în ceea ce priveşte echipamentul modern, atitudinea profesionistă şi banii). Drept urmare, guvernul trebuie să folosească mulţi subcontractori. Acest lucru duce de cele mai multe ori la o mai bună pregătire (cu costuri mari), dar nu rezolvă problema programatorilor cărora nu le place să aibă de a face cu atitudinea rezervată a organizaţiilor guvernamentale la adresa dezvoltării software-ului. Pe scurt, ASN întâmpină dificultăţi în a făcu un pas înaintea tehnologiilor de computer şi criptare disponibile pentru terorişti. Dar cel puţin ASN, în ultimii ani, a recunoscut că are această problemă. Nevoile războiului împotriva terorismului (de exemplu spargerea codurilor folosite de e-mailurile teroriştilor) creează premisele pentru inovare şi iniţiativă în cadrul ASN.

LIPSĂ DE INFORMARE ÎN GESTIONAREA INFRACŢIUNILOR

Programatorii au avut întotdeauna de a face cu un management defectuos. Acest lucru începe să se schimbe întrucât managerii cu ceva experienţă urcă în ierarhia corporaţiilor. Cu toate acestea, nebunia.com de la sfârşitul anilor ’90 nu a ajutat la nimic. În 2000, firma de securitate corporativă Kroll Associates emitea cecuri pentru 17 directori şi membri din conducerea companiilor de internet. S-a dovedit că 39% dintre aceştia fuseseră găsiţi vinovaţi de fraudă, nu declaraseră un jaf bancar ce avusese loc de curând, violaseră tot soiul de legi şi se asociaseră cu organizaţii criminale. Astfel de probleme nu sunt neobişnuite în rândul directorilor de companii, dar Kroll a evidenţiat că procentul acestora din companiilor neconectate la internet este de zece la sută. Domeniul.com era atât de plin de oameni care nu ştiau ce fac, încât răufăcătorii au profitat de această oportunitate şi au intrat

imediat în scenă. Acest lucru avea implicaţii serioase pentru securitatea internetului. De exemplu, companiile noi sunt cele mai predispuse la a face greşeli în ceea ce priveşte această zonă. Cu atât de multe probleme de rezolvat înainte de a începe, nu se acordă prioritate securităţii din timpul navigării pe internet. Acest lucru se petrece mai ales atunci când conducerea companiei este formată din persoane care nu au prea multe cunoştinţe despre internet.

Multe, cornuri care au murit şi unele care au supravieţuit au suferit drept urmare spargeri jenante (şi de multe ori scumpe). Cele mai devastatoare spargeri au fost cele în care s-au furat cărţi de credit sau informaţii despre clienţi. În unele cazuri, sute de mii de informaţii despre numere de cărţi de credit au fost furate. Vestea despre site-uri conduse de manageri care nu dădeau doi bani pe securitate s-a răspândit rapid printre hackerii black hat. Drept urmare, astfel de site-uri au fost atacate frecvent.

VORBEŞTE CU JUDECĂTORUL

Departamentul Apărării încearcă să îi prindă şi să îi aresteze pe cei care le atacă site-urile. În mare parte, se face asta pentru a-i descuraja pe alţii şi pentru a da un exemplu. Cea mai mare parte din cei prinşi sunt adolescenţi. Pentru că mai degrabă sunt o pacoste, armata încearcă să recupereze cel puţin costurile de prindere a hackerului şi de reparare a pagubelor. Aceste costuri pot fi de la 100.000 $ până la câteva milioane pentru fiecare incident. Sistemul juridic american face de multe ori dificil acest lucru. Există un caz care demonstrează asta. În 1999, Departamentul Apărării l-a prins pe Chad D. Davis atacând un site web al armatei SUA. A pledat vinovat pe 5 ianuarie 2000. Armata dorea să îşi recupereze pierderile. Dar judecătorul a fost de acord să ia în considerare declaraţia apărării conform căreia armata nu reuşise să ia măsurile necesare pentru a proteja serverul şi să ţină cont de acest lucru atunci când va stabili costurile totale. S-a

dovedit că, deşi armata remediase punctele vulnerabile ale serverelor, acel server în cauză nu fusese reparat. Armata ştia despre această problemă şi chiar luase măsuri cu ceva vreme înainte. Dar când site-ul fusese mutat pe serverul actual, administratorul de sistem responsabil a neglijat instalarea noilor programe. Acest lucru i-a permis lui Davis să intre şi să înlocuiască materialul armatei cu un mesaj care anunţa spargerea. Judecătorul a declarat armata vinovată pentru că nu a luat măsuri de precauţie într-o problemă de care avea cunoştinţă.

CYBER-RĂZBOINICI ÎN REZERVĂ

Departamentul Apărării pierdea cyber-războinici instruiţi în timpul nebuniei, corn de la sfârşitul anilor ’90, şi încerca să compenseze această realitate nedorită prin alcătuirea unor unităţi de cyber-război. Instruirea soldaţilor pentru a ataca şi proteja site-urile de internet era costisitoare. Dar aceste trupe puteau face mult mai mulţi bani folosindu-şi abilităţile în civil. În cele din urmă, în 2001, cineva şi-a dat seama că asta nu era unica problemă. Întotdeauna existase un deficit de oameni bine pregătiţi din punct de vedere tehnic în domeniile care pe piaţa de muncă civilă erau la mare căutare (programatori şi operatori de toate felurile). De aceea, soluţia, aşa cum a fost dezvoltată în ultimele decenii, era de a acoperi aceste lipsuri prin formarea unor unităţi de rezervă specializate. Armata nu îi putea împiedica pe oameni să plece, dar se putea juca cu ei inducându-le sentimentul de vinovăţie şi astfel îi convingea să se înscrie într-o unitate de rezervă. Multe trupe au făcut acest joc. Dădeau dovadă de patriotism, făceau un ban în plus şi, dacă ar fi izbucnit un război, puteau lua parte la el. Acest lucru le-a surâs în mod deosebit cyber-războinicilor. Practica pe care o făceau pe timp de pace era captivantă, dar în vreme de război ştiau că vor avea parte de şi mai multă acţiune, de multe ori umăr la umăr cu cei mai buni hackeri ai naţiunilor duşmane.

De asemenea, existau şi alte avantaje. Deşi „rezerviştii” ar fi lucrat pentru armată numai o lună pe an, ar fi fost suficient de mult pentru a-i ţine la curent cu ceea ce puneau la cale trupele cyber-războinice active. Mai mult, rezerviştii puteau veni cu cele mai noi instrumente şi tehnici ale internetului civil.

Fără aceşti cyber-războinici de rezervă, armata ar fi trebuit să apeleze la consultanţi civili la vreme de război. În mijlocul unei situaţii urgente, civilii, oricât de buni ar fi fost, erau nevoiţi să înveţe ce făcea armata. Pe lângă timpul petrecut pentru acest lucru, se verificau şi trecutul şi cazierele acestora. Armata mai avea şi opţiunea de a angaja rezervişti în calitate de contractori civili pentru unele proiecte. Astfel se economiseau bani inclusiv pentru instruire (despre metodele de operare ale armatei).

Şi apelul la patriotism şi mândrie naţională a dat rezultate. Unităţile de rezervă cyber-războinice au avut un mare succes în procesul de recrutare. Pe lângă recrutarea cyber-războinicilor militari care plecau, oferta era valabilă pentru toţi tinerii care activau în domeniul securităţii pe internet. Departamentul Apărării are deja cinci unităţi de rezervă (cu un total de 182 de cyber-războinici extrem de bine pregătiţi) şi plănuieşte să ajungă la 600 până în 2007. Şi atacurile din 11 septembrie au ajutat la procesul de recrutare.

SIMULAREA PRESEI

Jandarmii armatei americane (în număr de 2.200) sunt consideraţi infanteria de elită a acesteia. Antrenamentele sunt intense, dar nu se mai limitează numai la luptă. În ultimii ani, tot mai multe exerciţii au inclus ipoteza că de multe ori ziariştii vor fi prezenţi pe câmpul de luptă. De aceea jandarmii învaţă cum să aibă de a face cu jurnaliştii care ajung în mijlocul luptei sau sunt deja acolo când soseşte armata. Acest lucru s-a întâmplat deja în timpul unor misiuni pe timp de pace. Jandarmii mai

tineri nu sunt tocmai încântaţi, dar îşi dau cu toţii seama că un câmp de luptă modern este de multe ori plin de oameni din presă şi că această problemă trebuie rezolvată. Războiul informaţional a devenit crucial pe măsură ce reportajele din mass-media au început să fie transmise în timp real. Acum, jurnaliştii stau departe de câmpul de luptă şi folosesc telefoane prin satelit şi aparatură care le permite să raporteze, în timp real, cu ajutorul camerelor video de calitate. Luptătorii trebuie să ştie cum să facă faţă acestei situaţii. Dacă spui ceva nepotrivit la momentul nepotrivit şi adaugi şi un film ce te poate induce în eroare, vei fi nevoit să îţi asumi pierderea cyber-războiului. Orice va ajunge la ştirile TV se va răspândi pe internet în fiecare colţ al lumii în numai câteva ore. Cel care a făcut gafa îşi va da seama că localnicii, care până atunci erau prietenoşi, nu vor mai fi chiar la fel şi poate vor trage şi în el. În cyber-război nu se folosesc gloanţe, dar în mod sigur se va apela la ele în foarte scurt timp.

PARTEA ÎNTUNECATĂ A UTILIZĂRII SITE-URILOR MILITARE

Departamentul Apărării a fost întotdeauna preocupat de OPSEC (de securitatea operaţională). Adică, aşa cum spune armata, de „procesul de ascundere faţă de inamici a informaţiilor despre capacităţi şi/sau intenţii prin identificarea, controlarea şi protejarea probelor de obicei neclasificate despre planificarea şi executarea activităţilor susceptibile”. Asta înseamnă că informaţiile militare sunt foarte bine controlate. Atunci când a fost lansat World Wide Webul oamenii responsabili de OPSEC şi-au dat seama în scurt timp că au de-a face cu o problemă majoră.

Trupele au abordat webul cu entuziasm şi au început să creeze site-uri pentru unităţile proprii. Mândria a fost întotdeauna un mijloc important de a întări moralul şi de a păstra buna dispoziţie a trupelor (şi a familiilor lor). Ideea unei pagini web pentru o unitate s-a răspândit mai repede

decât un incendiu. Pe aceste pagini erau postate nume şi informaţii biografice despre trupele din unitate, cu ce se ocupa unitatea în momentul respectiv şi tot felul de lucruri de interes pentru trupele din unitate, dar şi pentru teroriştii şi naţiunile străine care la un moment dat s-ar putea lupta cu astfel de unităţi. În acest punct, aşa cum au descoperit ofiţerii responsabili de OPSEC, bunele intenţii au şi o parte întunecată.

Nu a trecut mult timp până când agenţiile secrete au descoperit că inamici reali sau potenţiali au început să se conecteze la site-urile militare. Aici exista o sursă foarte mare de informaţii despre armata americană, actualizată în mod regulat de propriile trupe care făceau asta cu mândrie. Paginile unităţilor erau atât de populare încât acestea pur şi simplu nu au putut fi interzise. Chiar dacă s-ar fi apelat la aşa ceva, civilii (care erau de multe ori la dispoziţia trupelor) le-ar fi putut reînfiinţa în altă parte. Mai mult, o mare parte din informaţiile de pe pagina unităţii erau disponibile oricui umbla prin baza militară şi accesa paginile de noutăţi sau citea ziarul unităţii. Totuşi, accesul acesta atât de uşor a salvat timpul şi banii de călătorie ai răufăcătorilor dând în acelaşi timp mari dureri de cap responsabililor de OPSEC care se şi închipuiau puşi la zid de reprezentanţii Congresului.

De aceea armata a răspuns aşa cum face de obicei în astfel de situaţii, a emis reguli şi îndrumări pentru paginile web militare (oficiale şi neoficiale, întrucât mare parte din aceste pagini erau create din iniţiativa trupelor în timpul liber şi cu propriile resurse). În primul rând, nu aveau să mai fie postate informaţii considerate în mod normal confidenţiale sau clasificate. Aici erau incluse planificarea mişcărilor trupelor sau operaţiuni care nu fuseseră anunţate oficial. De asemenea, a devenit ilegală postarea diferitelor informaţii personale detaliate (adresa sau numărul de telefon al militarilor, de exemplu). Chiar şi înainte de 11 septembrie 2001, astfel de date erau

considerate folositoare de către teroriști.

Aceste restricții nu au ridicat nemulțumiri în rândul militarilor și al familiilor lor. Dar aveau noimă pentru cei din armată. Mai important decât atât este că armata nu a încercat să se amestece în e-mailurile trupelor. De fapt, acestea erau încurajate. Chiar și marinarii și în special cei din submarine aveau acces la acest serviciu. E-mailul era un puternic factor de creștere a moralului trupelor, mai ales în cazul celor care erau separați de familie timp de mai multe luni. E-mailul devenise extrem de popular dat fiind că multe trupe erau trimise în misiuni de menținere a păcii în zone izolate, locuri unde nu puteau fi însoțite de familii. Militarii erau încântați pentru că acest moral ridicat făcea ca unitățile să fie mai fericite și să dea mai mult randament. Acest lucru a păstrat tot mai mulți oameni în armată. Era foarte trist că tot mai multe persoane părăseau armata de fiecare dată când contingente însemnate erau trimise în misiuni de păstrare a păcii pentru un timp îndelungat și în locuri izolate.

Dar nici e-mailul nu era scutit de problemele OPSEC. Deși trupele erau avertizate să nu discute pe e-mail despre informații delicate sau clasificate, nu exista nicio modalitate simplă de a împiedica acest lucru. Celor de pe nave sau din locuri izolate unde armata oferea conexiune la internet li se scanau e-mailurile automat în căutare de astfel de informații. Orice mesaj suspect ar fi fost blocat, fiind acuzat de violarea OPSEC. Dacă mesajul era curat, acesta pleca mai departe. Dacă nu, expeditorul era contactat și era consiliat în materie de OPSEC. Orice cont de e-mail, mii era scanat. Cu toate acestea, multe trupe aveau conturi de e-mail nonmilitare. Unii procedau astfel pentru că preferau, la fel ca mulți civili, să separe e-mailurile de la serviciu de cele personale. Alții o făceau pentru că uneori e-mailului militar i se crea o copie în timpul procesului de monitorizare. Un alt motiv era, desigur, faptul că multe trupe nu erau de acord să li se

monitorizeze mesajele. Chiar dacă software-ul era cel care scana, rămâneau totuşi americani, iar americanii iau intimitatea mai serios decât multe alte naţiuni.

Lucrurile devin şi mai rele. Cei de la OPSEC au supravegheat iniţial chaturile militare. Altele sunt folosite de subordonaţi ai celor din armată. Toată lumea vorbea despre chestiuni profesionale, iar lucrurile spuse de ei îi aduceau de multe ori pe cei de la OPSEC pe culmile disperării. Odată, un tânăr administrator militar de sistem, în încercarea de a găsi modalităţi de a face serverul navei pe care se afla mai sigur, a fost surprins descriind detalii tehnice despre securitatea serverului pe un chat. Marinarul nu încerca decât să obţină nişte sfaturi tehnice gratuite, dar oricine din cei care se aflau în acel chat ar fi putut lua notiţe. Instituţiile legale şi agenţiile de informaţii secrete care monitorizaseră chaturi de tot felul s-au împiedicat de multe violări ale OPSEC precum aceasta. Nu se puteau face prea multe lucruri, cu excepţia accesării acestor chaturi prin conturile militare pentru că armata are software care identifică cine ce spune. Era nevoie de mai multă consiliere OPSEC.

Şi flota este îngrijorată cu privire la scurgerile de informaţii întrucât navele au acum acces la internet. Pentru protecţie dar şi pentru elementul de surpriză, flota depinde de neidentificarea navelor ei atunci când se află în largul mării. Unii marinari au fost deja prinşi dezvăluind date despre locaţia în care se află în timpul conversaţiilor de pe chat.

Un scenariu cu privire la care flota este îngrijorată e ca nu cumva teroriştii să afle adresa familiei unui marinar de pe o pagină web, să răpească un membru al familiei şi să facă apoi presiuni asupra marinarului pentru a da informaţii. Deşi acest scenariu poate părea un pic forţat, toată lumea îşi dă seama acum că avem de-a face cu o generaţie de terorişti nemiloşi, cu imaginaţie bogată. Teroriştii actuali s-au folosit deja de răpiri pentru a forţa

soldaţii să spioneze în folosul lor.

Nu există soluţii uşoare pentru niciuna din aceste probleme. Pentru moment, armata trebuie să pună în balanţă avantajele unei pagini web şi eventualitatea unor noi pericole.

CUM SĂ SPARGI O REŢEA FĂRĂ CALCULATOR

Unele forme de hacking sunt extrem de periculoase şi nu necesită niciun fel de cunoştinţe despre programare. De exemplu, se poate obţine (cu ceva efort şi vreo 500 $) un radio care operează pe frecvenţele folosite de turnurile de control ale aeroporturilor. Din moment ce aceste radiouri sunt portabile, impostorul se află de obicei într-o maşină şi se deplasează permanent astfel încât să fie greu de prins chiar şi de o echipă de poliţie. Deşi hackerul din acest caz nu are nevoie de cunoştinţe despre computere, ar trebui să poată înţelege procedurile de control al traficului aerian. Într-o astfel de situaţie, este posibil să direcţionezi două sau mai multe aeronave într-un punct în care să se producă o coliziune în aer. Oricare ar fi motivele, forma aceasta de vandalism este mai populară în Marea Britanie, unde numărul acestui fel de incidente a ajuns de la trei în anul 1998 la peste 20 în anul 2000.

Există unul sau două cazuri serioase pe an în SUA, iar vinovaţii sunt de cele mai multe ori prinşi şi întemniţaţi. Activitatea din Marea Britanie se pare că este opera a numai trei indivizi şi niciunul nu pare a fi terorist. Un motiv pentru incidenţa mai mare a „detectării avioanelor” (reţinerea numerelor de identificare ale avioanelor şi un interes mare pentru operaţiunile aeroportului) este popularitatea de care se bucură. Trebuie menţionate două lucruri. Pentru a duce la bun sfârşit un atac eficient este nevoie de echipament şi informaţii tehnice. În al doilea rând, datele şi echipamentul sunt de multe ori uşor de găsit.

CAPITOLUL 8 CYBER-RĂZBOINICII
Termeni tehnici

Glosarul complet, ce include şi termenii definiţi mai jos, poate fi găsit la sfârşitul cărţii.

CERT – Computer Emergency Response Team1, fondată iniţial de Departamentul Apărării SUA în 1988 pentru a analiza rapid înşelătoriile sau dezastrele majore de pe internet. CERT operează în afara Universităţii Carnegie Mellon şi încă mai este principala instituţie internaţională pentru rezolvarea problemelor de pe internet.

CIC – Combat Information Center2. Inventat în timpul celui de al Doilea Război Mondial, când au apărut o mulţime de senzori electronici (radar, aparate de sunet) şi părea o idee bună să trimiţi toate aceste informaţii către o încăpere mare (de pe o navă sau un buncăr) unde aveau să fie sortate, puse pe hărţi şi ecrane pentru a putea fi asimilate de comandanţii care luau deciziile. În ziua de azi, CIC-urile sunt camere pline de monitoare de calculator. La un moment dat, CIC a devenit o sursă pentru descrierile science-fiction despre cum ar trebui să arate „puntea unei nave spaţiale”.

Perioada de luare a deciziei este timpul de care ai nevoie ca să recunoşti informaţiile, să îţi dai seama la ce se referă, să iei o decizie şi să o pui în practică. În termeni militari, pilotul sau comandantul unităţii de infanterie care are cea mai scurtă perioadă de luare a deciziei va câştiga. Aceste perioade joacă de asemenea un rol în crearea software-urilor şi combaterea infracţiunilor pe internet. Viteza contează.

ASN [National Security Agency (Agenţia pentru Siguranţa Naţională din SUA)] – Este o organizaţie secretă (în timpul Războiului Rece, guvernul nici măcar nu

recunoştea că există) care dezvoltă coduri secrete (criptare) pentru a păstra secrete comunicaţiile americane confidenţiale. ASN se ocupă de asemenea şi cu dezlegarea codurilor inamicilor (decriptare). Utilizarea tot mai mare a criptării pe internet a atras o mare parte din atenţia ASN.

NIPC este Naţional Infrastructure Protection Center3. A fost înfiinţat de către FBI pentru a supraveghea prinderea infractorilor pe internet.

NIPRNET este o structură a Departamentului Apărării care are numai câteva conexiuni la internetul obişnuit.

SIPRNET este o structură secretă a Departamentului Apărării care trimite toate informaţiile folosind criptarea (codarea) şi nu este conectată la internetul pe care noi ceilalţi îl folosim.

Red Attack (sau Echipa Red ori Echipa Tiger) constă într-un grup de experţi în internet care îţi va sparge sistemul pentru a vedea cât de bună este apărarea pe care o ai. Acest lucru poate fi costisitor (începe de la 5.000 $ şi ajunge rapid la şase cifre), în funcţie de cât de mare este sistemul.

Hai să discutăm despre lucrurile de bază.

Cine sunt cyber-războinicii? Sunt trupe care chiar duc lupta pentru informaţii. Nu orice informaţii, ci date care joacă un rol crucial şi care stabilesc cine va câştiga şi cine va pierde. Adică se referă la majoritatea trupelor de luptă. Navele de război, tancurile şi avioanele de luptă operează în grupuri unite unele cu celelalte în reţele de informaţie. Sediile centrale primesc atât de multe date încât un obiectiv important este sortarea lor suficient de rapidă pentru a fi utile. Dar noi ne vom concentra asupra cyber-războinicilor care apără ei înşişi reţelele şi le atacă pe ale inamicului. Reţeaua principală este internetul, dar sunt şi multe altele mai mici.

Cine are armate de cyber-războinici? SUA, China, Rusia, Japonia, Coreea de Sud şi majoritatea naţiunilor

europene au organizat unităţi speciale pentru atacarea şi apărarea internetului şi a reţelelor mai mici. Ţările mai mici văd aceste eforturi ca pe un mod de a nivela terenul de joacă pentru atunci când se vor confrunta cu un duşman mai mare. SUA sunt privite ca fiind vulnerabile în mod special în faţa atacului cyber-războinic, pentru că americanii folosesc cel mai mult internetul.

Care dintre aceste forţe este mai periculoasă şi cine se pricepe mai mult sau mai puţin la cyber-război? SUA au cele mai impresionante forţe de cyber-războinici, dar China a declarat în mod public că vede cyber-războiul ca fiind cea mai puternică armă a sa într-un viitor război cu America.

De ce a devenit internetul câmp de luptă? Ideea de a folosi internetul pe post de câmp de luptă este parte dintr-un concept mai amplu, numit război informaţional. Ideea de bază este că nu numai internetul, ci şi informaţiile în general sunt cheia spre eficacitatea forţelor armate. Astăzi avem parte de mult mai multe informaţii şi acela care deţine mai multe şi ştie cum să le folosească va câştiga orice război viitor. Ducerea lui pe internet sau pe orice alt fel de reţea este doar o parte a acestei bătălii pentru informaţii

VA FUNCŢIONA CYBER-RĂZBOIUL?

O mare parte din ceea ce se poate face cu cyber-războiul constă doar în speculaţii, în parte pentru că în mod constant apar noi echipamente şi tehnologii şi pe de altă parte pentru că de abia de curând au început strategii militari să ia în considerare şi acest aspect ca o nouă formă de război. Gândeşte-te: ideea de a folosi computerele peste tot este recentă. Computerele au fost inventate în timpul celui de al Doilea Război Mondial „când existau numai câteva. Ele au avut puţin de a face cu Războiul din Vietnam din anii ’60. De abia în timpul Războiului din Golf din 1991 s-a conturat conceptul de

„cyber-războinic”. În anii ’90 a avut loc o explozie a folosirii PC-urilor şi a reţelelor. Înainte de această perioadă „ele erau utilizate numai de maniaci şi de oamenii de afaceri cutezători.

Principala reţea era cea deţinută de companiile de telefonie. La sfârşitul anilor ’90, lumea se schimbase. Toată lumea ştia ce este un PC, cei mai mulţi dintre noi aveau unul şi erau conectaţi la internet. La fel şi majoritatea companiilor, agenţiilor guvernamentale şi unităţilor militare. Niciun sistem de comunicaţii în masă de dinainte nu se mai dezvoltase atât de repede. La scurtă vreme s-a descoperit că experienţele din trecut nu erau prea folositoare. Sau erau?

Cyber-războinicii pot fi găsiţi ascunşi în sediile centrale pline de monitoare şi tehnicieni talentaţi care furnizează comandaţilor ultimele informaţii despre cine (sau ce) apare sau dispare de pe ecran. Este de fapt povestea mai veche de 50 de ani despre radare şi operatori de sunet care îşi folosesc echipamentul pentru a afla unde se află inamicul şi ce pune la cale. Numai că este la scară mai mare, cu mult mai multe aparate electronice conectate între ele şi conduse din acelaşi loc. Flota SUA a început să folosească aşa ceva acum 60 de ani. Au numit această structură CIC (Combat Information Center). Pe atunci nu aveau decât radare, sonare şi multe radiouri pentru a comunica cu alte nave sau avioane. La vremea respectivă era tehnologie avansată. Dar numărul aparatelor electronice a crescut tot mai mult atât în calitate, cât şi în cantitate. Armata şi forţele aeriene au adoptat şi ele abordarea CIC a flotei. La apariţia internetului, era evident că fiecare unitate avea nevoie de un CIC. Nu numai fiecare unitate, dar de multe ori şi maşinile de luptă individuale precum avioanele şi tancurile de atac. Când am intrat în secolul XXI, nu mai era vorba doar de război, era cyber-război.

RĂZBOIUL INFORMAŢIONAL ATUNCI ŞI ACUM

Războiul informaţional a început ca unul dintre acele concepte ce provocau agitaţie în anii ’90 prin armată şi guvern. De fapt, este o farsă de marketing. Iar o mare parte dintre lucruri au existat de multă vreme, dar acum sunt prezentate astfel încât să fie mai uşor să obţină bani de la plătitorii de taxe. În timpul anilor ’90, sute de organizaţii militare şi guvernamentale diferite şi-au modificat misiunea pe care o aveau pentru a se implica în războiul informaţional. Războiul informaţional înseamnă să faci ceea ce ai făcut întotdeauna, dar mai rapid, cu ajutorul computerelor şi al reţelelor de informaţii (precum telefoanele mobile şi internetul). Pe scurt, războiul informaţional nu este ceva nou. Ideile de bază au existat de mai multe mii de ani, dar versiunea actuală ce foloseşte înalta tehnologie este funcţională de aproape un secol.

Din moment ce războiul informaţional înseamnă o grămadă de ţări amestecate într-o nouă bătălie, a apărut într-un nou mod de luptă formidabil: cyber-războiul. De multe ori, cele două noţiuni se suplinesc una pe alta, dar ambele acoperă multe operaţiuni distincte. Acestea includ noţiunile prezentate în următoarele paragrafe:

Comandarea şi conducerea războiului – să acţionezi în aşa fel încât să îngreunezi comunicarea şi controlul inamicului asupra forţelor sale de luptă. Este un principiu antic de război. Totuşi, este poate cel mai eficient aspect militar al războiului informaţional. Cheia este să fii în stare să iei decizii mai repede decât oponentul tău şi apoi să le pui în practică. Acest lucru se referă la scurtarea timpului necesar pentru luarea unei decizii. Sau, aşa cum îi place armatei să spună, „să întrerupi ciclul decizional al inamicului”. Nu ar trebui să existe nimic misterios cu privire la acest timp, este un aspect al vieţii. Tot ce facem se învârte în jurul acestui aspect. Armata a creat un acronim: OODA (observă ceva, orientează-te în funcţie de ceea ce s-a întâmplat, decide cum să reacţionezi,

acţionează). Timpii de luare a unei decizii nu sunt diferiţi în viaţa civilă. De exemplu, dacă vezi un anunţ pentru un nou loc de muncă, dar întârzii mai mult timp cu trimiterea candidaturii faţă de altcineva la fel de calificat pentru slujbă, atunci nu ai noroc (altcineva va obţine postul).

Totuşi, războiul informaţional ne poate împiedica să observăm. Dacă nu avem acea informaţie nu ne putem orienta cum trebuie, nu putem lua o decizie şi, cel mai important, nu putem acţiona. De exemplu, să presupunem că un expert în computere a intrat într-una din reţelele care ajută la adunarea informaţiilor secrete pentru SUA. Hackerul inamic a şters unele informaţii şi a modificat unele date, creând o imagine greşită a ceea ce se întâmplă pe câmpul de luptă. Acestea fiind făcute, comandanţii americani vor observa o versiune greşită a realităţii şi vor ajunge să ia decizii dezastruoase. Consecinţa: bombardarea zonelor unde se presupune că se află rezervele de muniţie şi vehiculele inamicului, dar în care, de fapt, se află tabere de refugiaţi. Înţelegi?

Securitatea operaţională. Numită OPSEC (OPerational SECurity) de oamenii din armată. Se referă la împiedicarea duşmanului să pună mână pe informaţii utile. Nevoia de OPSEC a generat sloganuri precum cele din cel de al Doilea Război Mondial: „Gurile slobode scufundă navele” şi „Duşmanul ascultă”. OPSEC supraveghează informaţiile secrete. Înseamnă să te asiguri că documentele secrete sunt bine depozitate, iar mesajele electronice sunt codate sau nu sunt uşor de citit de către inamic. Mai înseamnă şi să instruieşti trupele să protejeze informaţiile importante pentru ele.

Războiul electronic. Se referă la folosirea mijloacelor electronice în anticul joc al înşelătoriei. Începând cu telegraful intrat în uz în 1850, războiul electronic a ajuns să conteze în al Doilea Război Mondial, iar acum este o parte standard din arsenalul oricărui războinic profesionist. Dezvoltarea războiului electronic se

pliază pe istoria tehnologiei din ultimii 150 de ani. De la invenţia telegrafului din 1850, în anii 1870 a apărut telefonul, apoi radioul în jurul anului 1900, sonarul în 1906 şi radarul în anii ’30. În timpul celui de al Doilea Război Mondial au fost dezvoltate cele mai multe arme electronice pe care azi le avem (bombele inteligente, contramăsurile electronice, AWACS, CIC, computerele şi reţelele). Practic, ultimii 60 de ani i-am petrecut îmbunătăţind armele electronice pe care le-am inventat în cel de al Doilea Război Mondial.

Întărirea. Înseamnă creşterea rezistenţei aparatelor electronice la EMP (pulsul electromagnetic). Unul dintre efectele secundare ale războiului nuclear este EMP-ul. Este un val de înaltă energie care distruge sau avariază microelectronicele (adică totul, de la echipamentul militar la telefoane mobile, televizoare şi PC-uri). Adaugă cinci sau zece procente la costurile unui microcip şi îl poţi ţine departe de efectele EMP. Nu există o protecţie maximă, dar e suficient de bună pentru guvern. Şi doar pentru că este puţin probabil ca armele nucleare să fie folosite, nu înseamnă că poţi ignora EMP-ul, întrucât există un număr tot mai mare de aparate care pot genera un EMP distrugător fără o explozie nucleară. Aceste generatoare de EMP sunt văzute ca o posibilă armă nimicitoare. Treci cu un camion (în care se află un generator EMP) pe lângă Pentagon sau pe Wall Street şi eliberează o doză de energie electromagnetică. Majoritatea PC-urilor şi a aparaturii electronice pe o rază de o sută de metri vor deveni nefuncţionale. Mai mult, date importante se pierd, iar operaţiunile vor merge foarte prost până când echipamentul va fi înlocuit şi toate defecţiunile reparate. Cele mai multe electronice din echipamentul militar sunt întărite, dar majoritatea PC-urilor folosite de armată şi de companii nu sunt.

Hackerii. Aceştia sunt oamenii care se pot conecta pentru a provoca pagube pe internet folosind nimic mai

mult decât un PC. Acesta este un război de gherilă în care aproape oricine, de oriunde din lume, se poate implica. Nu ai nevoie decât de un computer, un modem şi ceva hotărâre. Este ceva nou pentru că de abia au fost formate reţelele de computere internaţionale pe care le poate accesa aproape oricine. Internetul este cel mai bun exemplu în acest sens. O mare parte dintre programatorii plictisiţi sau alţi oameni care au mult timp la dispoziţie şi răutate în suflet navighează pe internet căutând-o cu lumânarea. Acest lucru se întâmplă de decenii. De asemenea, au loc multe înşelătorii pe reţelele din cadrul companiilor. Puţine infracţiuni, dar multe înşelătorii. S-au făcut câteva încercări, în ultimul deceniu, de a transforma problema hackerilor într-o armă militară. Nu a fost uşor. Înşelătoria nu este întotdeauna o armă utilă. Dar rezultatele pot fi spectaculoase dacă reuşeşti să-l introduci pe unul dintre cyber-războinicii tăi într-o reţea inamică în timpul războiului. Acest lucru nu s-a întâmplat decât în ficţiune, dar multe naţiuni încearcă din greu ca în viitor să fie ceva real.

Blocajul informaţiilor. Acesta este o variantă a practicii antice de a bloca accesul navelor cu provizii pe teritoriul inamic. Cum datele de acum sunt foarte importante, nimeni nu poate închide sateliţii, legăturile prin cablu sau turnurile de antene cu unde de înaltă frecvenţă care transmit date către teritoriul inamic. Uneori le poţi opri pentru că le controlezi (compania care furnizează acces telefonic pe distanţe mari, să zicem, Irakului, poate fi convinsă să oprească accesul Irakului la reţeaua internaţională de telefonie). Vor exista efecte secundare după o vreme, mai ales în zonele cu mai multă tehnică. Operaţiunile bancare internaţionale, internetul şi comunicaţiile de tot felul depind de aceste reţele la mare distanţă. Desigur, ţările pot folosi radioul. Dar acesta este limitat şi nu poate înlocui cu adevărat sateliţii de comunicaţie şi cablurile cu fibră optică.

Războiul bazat pe informaţii. Cum radioul şi televiziunea au devenit mass-media, în anii ’60 a devenit clar că mass-media electronică poate avea un efect decisiv asupra opiniei publice şi a luării deciziilor politice. Chiar şi înainte de asta, tiranii de toate felurile (mai ales naziştii şi comuniştii) şi-au dat seama cât de important este să deţii controlul mass-media (mai ales al celei scrise) şi să o foloseşti pentru propriile nevoi. Prin controlarea mass-media, tiranii puteau scăpa nevinovaţi pentru uciderea în masă. Pe măsură ce tot mai mulţi au început să înţeleagă cum funcţionează mass-media în colectarea şi distribuirea informaţiilor, tot mai mulţi oameni au participat la crearea şi influenţarea a ceea ce trece drept ştire. Grupurile de presiune au înţeles de asemenea că dacă pot genera publicarea unui anunţ de presă, vor atrage atenţia directorilor de ştiri radio şi TV şi îşi pot face mesajul cunoscut mai uşor (şi ieftin). Exemple excelente de războaie bazate pe informaţii au avut loc în timpul Războiului din Golf din 1991 şi al celui din Afganistan din 2001. Ştirile sunt considerate acum o armă şi sunt folosite ca atare.

Războiul psihologic. Este folosit de multă vreme şi se rezumă la răspândirea informaţiilor demoralizatoare şi eronate în tabăra inamicilor, încă este utilizat şi încă mai funcţionează. De asemenea, este mult mai uşor de purtat cu ajutorul internetului.

Dar mai trebuie luat în considerare un aspect al războiului informaţional. Acesta este definit în mare parte de modul în care foloseşti informaţiile ca armă împotriva trupelor inamice. Poţi bloca informaţia atunci când încerci să îţi ţii duşmanul în întuneric (prin distrugerea facilităţilor de transmisie radio şi televizată) sau poţi să te aperi de ea atunci când încerci să elimini informaţiile false pe care inamicul ţi le furnizează pe computer, telefon sau prin spioni. Se poate să preiei controlul asupra sistemului adversarului, cu tehnicile şi electronicele potrivite.

Tehnologia de care este nevoie într-un război informaţional include radarele de bruiere sau transmisiile radio (prin difuzarea multor „zgomote” electronice), dar şi reţelele de intruziune de înaltă tehnologie (viruşi sau atacuri DDOS care încetinesc anumite zone ale internetului) despre care citim în ziare şi ne temem că vor deveni mai utilizate în viitor. Războiul informaţional nu este ceva nou, numai că acum avem multe aparaturi şi tehnici care ne sporesc capacităţile şi numărul ţintelor pe care putem să le atacăm. Sporirea capacităţilor şi dependenţa de software şi hardware au crescut nevoia militarilor de a percepe ţintele războiului informaţional ca făcând parte din planurile de război. Căci dacă nu vor face acest lucru s-a constatat că duşmanul o va face. Dependenţa noastră tot mai mare de echipamentul electronic şi de internet a făcut ca războiul informaţional să nu mai fie doar un aspect al războiului, ci principalul aspect.

RĂZBOIUL DIN GOLF, PRIMUL RĂZBOI INFORMAŢIONAL

Războiul din Golful Persic din 1991 este de multe ori amintit ca fiind primul război informaţional. Ei bine, a fost şi nu a fost. Acel război a folosit mai multe elemente considerate ca făcând parte dintr-un război informaţional. Dar în acelaşi timp, nu s-a făcut nimic în acel război din ce nu se făcuse şi înainte.

Campania aeriană a fost deschisă cu un atac asupra sediilor centrale ale inamicului, a comunicaţiilor şi serviciilor vitale. Nimic nou până aici. Numai că în Războiul din Golf atacul a fost mai rapid şi mai complet decât în trecut. Nimic nou nici aici. De la al Doilea Război Mondial, conflictele ţărilor industrializate au fost mai rapide şi mai globale, învăţaseră din experienţă.

Coaliţia Războiului din Golf a dus o campanie de război psihologic asupra irakienilor care a fost remarcabil de eficientă, cel puţin dacă socotim viteza cu care s-au

predat irakienii atunci când forţele terestre ale Coaliţiei au apărut în vecinătatea lor. Nu este nimic nou nici aici. S-a mai întâmplat de câteva ori în ultimul secol. Era un război informaţional, în măsura în care erau aruncaţi fluturaşi deasupra trupelor irakiene în care li se spunea exact cum să se predea şi care puneau accent pe avantajele predării (deveneau oaspeţi ai saudiţilor şi nu erau omorâţi de americani).

Războiul din Golf a fost de asemenea în mare parte un război electronic, folosind metode vechi, deşi existau echipamente noi, care fuseseră inventate cu jumătate de secol mai devreme, în cel de al Doilea Război Mondial. Mass-media, de exemplu, era folosită foarte mult de ambele părţi pentru a influenţa opinia publică în timpul Războiului din Golf. Repet, aceasta era o tehnică având o lungă istorie în spate (de peste patru mii de ani).

A fost Războiul din Golf un război informaţional adevărat? Da, a fost. Şi succesul armelor şi echipamentelor de înaltă tehnologie folosite în conflict, plus tot mai marea agitaţie cu privire la hackeri au dus la folosirea denumirii de război informaţional, mai ales de către armată. A mai existat un motiv pentru care această denumire a devenit una la modă. Războiul din Golf şi Războiul Rece au luat sfârşit în acelaşi timp. Atunci când se termină războaiele, bugetul armatei este redus. Pentru a obţine mai mulţi bani, ai nevoie de un nou război. Când a apărut în scenă World Wide Web la mijlocul anilor ’90, nu era nevoie să fii un geniu în marketing (sau unul militar) ca să vezi că există pericole în creşterea rapidă a fenomenului internetului. Denumirea „război informaţional” a existat de multă vreme, dar când oamenii de le Pentagon au început să-l folosească pentru a descrie aspecte majore ale Războiului din Golf şi ale eventualelor războaie viitoare, a prins la public. Dintr-odată, atunci când era vorba despre vreo agendă sau o situaţie a bugetului care avea nevoie de ceva în plus pentru a deveni prioritară, nu era nevoie să spui

decât

„Război informaţional” şi banii începeau să curgă. Fiecare serviciu militar şi departament a căutat o definiţie a războiului informaţional care i-ar putea sluji pentru nevoile imediate sau obiectivele pe termen lung.

Dar până la sfârşitul anilor ’90, generalii au început să îşi dea seama că războiul informaţional era o ameninţare mult mai mare decât crezuseră, între timp, fiecare om din interiorul Pentagonului a realizat că cyber-războiul se poartă în „vreme de pace”. Într-adevăr, războiul informaţional se transformase în cyber-război. Imediat, armata şi-a dat seama că are nevoie de foarte mulţi cyber-războinici, şi asta rapid.

RĂZBOIUL INFORMAŢIONAL PE TIMP DE PACE

Utilizările tipice nonmilitare ale războiului informaţional se referă la spionii industriali şi economici care, fie că sunt liber-profesionişti, fie că lucrează ca agenţi guvernamentali, încearcă să câştige de partea lor un avantaj competitiv prin dezvăluirea secretelor inamicului şi protejarea acelora care aparţin angajatorului. Uniunea Sovietică a făcut acest lucru decenii la rând şi a avut destul de mult succes. Pe atunci nu se numea război informaţional, dar asta era de fapt. Şi poate avea un efect militar direct, dacă spionii tăi urmăresc tehnologia militară.

A mai existat un punct de vedere înşelător al războiului informaţional care a trecut în general neobservat timp de mai multe decenii. Gândeşte-te la efectul introducerii PC-urilor în munca experţilor din poliţie într-o ţară din lumea a treia. Experţii în computere introduc numele celor care sunt cunoscuţi ca fiind împotriva dictatorului local într-o bază de date. Dintr-odată, tiranul este mult mai eficient în a-i ţine sub control pe disidenţi. Este un război informaţional. Cei mai competenţi practicanţi ai războiului informaţional dus de

structurile de stat au fost comuniştii, iar ei au fost ultimii care au adoptat utilizarea computerelor. Uniunea Sovietică a demonstrat că încă mai poţi teroriza o mare parte din populaţie cu un index şi o bază de date primitivă, având control total asupra tuturor mijloacelor media. Un război informaţional clasic.

Nu ai nevoie de arme sau bombe pentru a duce un război informaţional. Desigur, pot fi folosite şi arme violente. După cum am văzut, majoritatea armelor folosite în acest tip de război au fost privite la început ca fiind nonviolente – de la redactarea ştirilor la colectarea rapoartelor despre vreme. Sunt simple date. Dar o mare parte din război este formată din date; chiar şi războinicii din triburile primitive care erau înarmaţi doar cu arcuri şi săgeţi erau conştienţi de valoarea datelor. Informaţii despre locul unde se află inamicul, cum luptă şi mediul din jurul câmpului de luptă în general. Poate că omul primitiv nu avea prea multă tehnologie, dar avea nevoie şi folosea foarte multe date. Altfel spus, cât de multe tipuri de triluri (folosite de multe ori ca semnale de către războinici) poţi identifica?

De la omul primitiv la cel modern, vedem una dintre diferenţele majore, şi anume numărul mult mai mare de date disponibile şi gradul mare în care depindem de date pe care nici măcar nu le înţelegem sau nu ştim că le avem. Ştii cât de multe date sunt transmise între componentele maşinii tale? Automobilele au acum microprocesoare şi sisteme de stocare a datelor. Fără ele, nu pot funcţiona. Hoţii au învăţat că radioul maşinii sau airbagul nu sunt la fel de valoroase precum computerul de bord. Mulţi şoferi îşi deschid maşina şi constată că a fost forţată portiera, computerul a fost deşurubat, maşina a rămas fără creierul ei, iar motorul nici măcar nu poate fi pornit. O formă de război informaţional este să foloseşti un dispozitiv electronic ce opreşte circuitele din computerul vehiculelor, făcându-l inutil (fie el vehicul civil, fie militar) şi fără să fie

lăsate urme vizibile. Aşadar, fie că furi, fie că dai peste cap computerul unei maşini, eşti implicat în războiul informaţional.

Dar pentru a crea sau a utiliza lucruri precum cele care distrug computerele maşinilor, ai nevoie de cyber-războinici.

Se poate spune că războiul informaţional include tot ceea ce faci pentru a păstra integritatea propriilor sisteme de informaţii în calea exploatării, modificării sau distrugerii, în vreme ce în acelaşi timp exploatezi, modifici şi distrugi sistemele de informaţii ale inamicului în procesul de obţinere a unui avantaj informaţional, în cazul în care se ajunge la o luptă armată. Aşa abordează Pentagonul războiul informaţional. Nu trebuie să foloseşti forţa ca urmare a acestui război. Dar ai nevoie de cyber-războinici şi în zorii secolului XXI Pentagonul şi-a dat seama că nu are nici pe departe suficient de mulţi.

Dar înainte de a recruta foarte mulţi cyber-războinici ai nevoie de un loc în care să îi pui să lucreze.

AUTORITATEA CYBER-RĂZBOIULUI AMERICAN

Pentagonul a primit un semnal de alarmă în timpul unui joc de război din 1997. Exerciţiul, numit „Receptorul eligibil”, a folosit hackeri white hat de la Agenţia pentru Siguranţa Naţională pentru a arăta cum este posibil, date fiind condiţiile actuale, să ataci elemente-cheie din economia americană. Hackerii au demonstrat că sistemele de control electric ale unor oraşe mari sunt şi ele vulnerabile în faţa unor intrări frauduloase similare. De asemenea, mass-media a pus accent pe modul în care exerciţiul a arătat cum poţi să spargi multe sisteme 911 şi să le opreşti. De fapt, aceşti hackeri ai ASN nu au distrus sistemul 911 prin accesul la internet, ci pur şi simplu au aranjat ca foarte mulţi oameni să sune la 911 în acelaşi timp şi să blocheze sistemul. Acest lucru putea fi făcut automat folosind computere care să apeleze încontinuu

911. Dar faptul că încă mai circulă poveşti despre „tipii care au spart sistemul 911” este un exemplu de război informaţional. Cu toate acestea.

„Receptorul eligibil” a speriat de moarte conducerea politică şi armata americană. Războiul informaţional nu mai era doar un truc de marketing al Pentagonului şi toată lumea îşi dorea cât mai mulţi cyber-războinici în timp scurt.

Aceste feste au arătat, de asemenea, că legăturile prin satelit prezintă şi ele riscuri. De multă vreme a fost recunoscut faptul că sateliţii sunt vulnerabili în faţa hackerilor, întrucât singurul mod de a trimite comenzi spre sateliţi este prin radio. Majoritatea comunicaţiilor de acest fel sunt făcute prin mesaje codate, dar aşa cum am văzut, codurile pot fi sparte sau pot fi obţinute de spioni. Oricum ar fi, nu afli despre asta până când nu izbucneşte un război şi dintr-odată fie altcineva a preluat sateliţii, fie i-a avariat. Acesta este un alt motiv pentru care militarii se tem atât de mult de

„Atacurile prin surprindere”. Şi nu numai sateliţii militari sunt în pericol. Există aproximativ 800 de sateliţi, majoritatea sunt civili, nu militari, şi ştim că sunt vulnerabili. De exemplu, în anii ’80, un hacker ce se autointitula „Captain Midnight” a preluat controlul asupra unui transmiţător (una dintre unităţile de transmisie/recepţie de pe un satelit) folosit de HBO şi a plasat acolo propriul mesaj. În 1999, a circulat un zvon neconfirmat despre un hacker care a preluat un satelit de comunicaţii militare într-o încercare nereuşită de şantaj. Tot în 1999, armata a decis să stabilească un singur sediu central care să se ocupe de cyber-război. Prima sarcină, desigur, a fost apărarea – pentru a rezolva toate acele vulnerabilităţi înspăimântătoare.

Comandamentul Spaţial al SUA (USSC) a fost (şi este) responsabil pentru sateliţii militari americani şi operaţiunile spaţiale. Aşadar, în octombrie 1999, a fost

însărcinat cu furnizarea instrumentelor procedurilor şi consilierilor meniţi să protejeze reţelele de computere ale Departamentului Apărării. Se făcea acest lucru pentru a preveni atacurile asupra reţelelor din partea hackerilor, teroriştilor şi criminalilor. De fapt, era vorba despre o restructurare birocratică. USSC a preluat o organizaţie deja existentă în cadrul Departamentului Apărării – JTF-CND4. La începutul anului 1999, JTF-CND a fost reorganizat după ce, aşa cum spune armata, „exerciţiile şi evenimentele reale au demonstrat nevoia unei singure agenţii de coordonare care să aibă autoritatea să conducă acţiunile necesare pentru apărarea reţelelor naţionale de computere de maximă importanţă". A fost recunoscut faptul că JTF-CND este „o soluţie interimară şi că sarcina va fi în cele din urmă desemnată unui comandament unificat".

JTF-CND al Comandamentului Spaţial a fost stabilit la sediul central al Agenţiei de Sisteme Informaţionale de Apărare (DISA5) şi cu un personal de aproximativ o sută de oameni operează în permanenţă pentru depistarea atacurilor majore ale hackerilor. Exista deja o reţea pentru depistarea intruziunilor şi monitorizarea sistemelor, iar acum cineva era responsabil pentru urmărirea lor şi organizarea unei apărări în cazul unui atac major. Aceasta este o procedură militară tipică şi destul de practică. Atunci când te confrunţi cu o nouă ameninţare, primul lucru pe care îl faci este să trimiţi avertizări atunci când tipii răi se îndreaptă spre tine.

Comandamentul Spaţial a stabilit patru niveluri de alertă, în funcţie de cât de periculoasă este ameninţarea cyber-războinică. Cel mai jos nivel de alertă este „Infocom Alpha", iar cel mai serios este „Infocom Delta". Atunci când este declarat un „Infocom Alpha", administratorilor de sistem ai Departamentului Apărării şi utilizatorilor li se comunică să schimbe parolele (în cazul în care cyber-războinicii inamici le-au furat pe cele existente), să

limiteze utilizarea telefonului mobil (sunt uşor de interceptat), să actualizeze cheile folosite pentru criptarea comunicaţiilor secrete (în cazul în care inamicul a decriptat cheile actuale şi adună toate informaţiile găsite), să facă o copie suplimentară a documentelor importante; personalul militar este îndemnat să actualizeze protecţia împotriva viruşilor de pe computerele de acasă, să revizuiască lista de control al securităţii şi, desigur, să raporteze activităţile suspecte. În timpul războiului „chinezo-american" dintre hackeri de la începutul anului 2001 (după incidentul EP-3), Comandamentul Spaţial a trecut la „Infocom Alpha". Procedurile pentru celelalte trei niveluri de alertă sunt secrete. Dar pornind de la ce se cunoaşte despre procedurile „Infocom Alpha", de la toată munca tehnică ce s-a efectuat, antrenamentele pentru nivelurile mai serioase de alertă vor avea nevoie de mult mai mulţi cyber-războinici. Poate de aceea detaliile sunt ţinute secret, pentru că ar fi evident că va fi nevoie de mai mulţi ani pentru recrutarea şi instruirea unui număr suficient de mare de cyber-războinici care să se ocupe de problemă.

Comandamentul Spaţial foloseşte două reţele internet private. Conduce afacerile prin NIPRNET (Non-classified Internet Protocol Router Network), care este reţeaua militară ce are unele legături cu internetul şi are peste două milioane de servere. Acestea sunt ţinta a circa o sută de intruziuni care au loc în fiecare zi. Majoritatea sunt script kiddies care se joacă, dar 10 – 20 dintre aceste încercări sunt destul de bine puse la punct pentru a necesita investigaţii suplimentare.

NIPRNET conţine o mulţime de date logistice (provizii, cereri de combustibil, muniţie şi altele asemănătoare) şi chestiuni legate de personal (adrese, numere de telefon şi chiar numerele cărţilor de credit). După 11 septembrie 2001, au fost stabilite mai multe restricţii în privinţa accesului la NIPRNET. încă mai puteai

trimite şi primi e-mailuri, dar pentru utilizatorii civili era mai greu să pătrundă.

Separat de NIPRNET, funcţionează SIPRNET (Secure Internet Protocol Router Network). Această reţea nu este conectată la internet (deşi funcţionează cu tehnologia internetului) şi îşi codează datele. Rareori este atacată şi spargerile sunt numai câteva, dacă nu chiar deloc (toate discuţiile despre atacurile asupra SIPRNET sunt clasificate). Reţeaua este folosită de armată pentru a discuta despre orice subiect secret. SIPRNET este disponibil peste tot în lume prin reţeaua de comunicaţii militare americane.

În octombrie 2001, Comandamentul Spaţial şi-a asumat responsabilitatea pentru războiul ofensiv de pe computere. Aici era inclusă şi dezvoltarea instrumentelor şi sistemelor de atac clasificate.

Comandamentul va dezvolta, testa şi grupa aceste instrumente ofensive pentru a fi folosite în războaiele viitoare. Această zonă este pusă la punct ca răspuns la faptul că singurul mod în care poţi construi un sistem de apărare aeriană în epoca cyber-războiului sau cel puţin unul care să aibă şanse să încetinească atacurile aeriene americane este prin folosirea reţelelor de computer. Acelaşi lucru se întâmplă şi pentru comandarea şi controlarea sistemelor necesare pentru forţele terestre şi navale. Astfel, accentul pus pe dezvoltarea armelor poate scoate din funcţiune sisteme similare. Deşi este un război mai puţin distructiv, prin folosirea semnalelor electronice în locul bombelor, este şi mai eficient. Nu se vrea a fi un „război fără arme”, analogul militar al „biroului fără hârtii”. Această formă de cyber-război se concentrează pe războiul informaţional. Prin distrugerea sau încetinirea capacităţii inamicului de a comunica, aduna şi analiza informaţii, armele lor devin mult mai puţin eficiente. Forţele aeriene practică acest lucru încă din cel de-al Doilea Război Mondial, prin utilizarea războiului electronic

menit să oprească apărarea antiaeriană a inamicului. Orbirea radarelor şi bruierea comunicaţiilor permit bombardierelor americane să ajungă la ţintele lor cu foarte puţine pierderi. Cyber-războiul extinde această formă de luptă pentru a include orice e conectat la internet sau oricare altă reţea electronică.

Ca întotdeauna, cheia către reţelele de arme eficiente este găsirea slăbiciunilor înainte ca utilizatorul inamic să o facă. Aşa cum am discutat, este o situaţie în continuă schimbare, întrucât administratorii de reţele străini îşi descoperă ei înşişi vulnerabilităţile şi le repară. Dacă un atac cyber-războinic eşuează din cauza aceasta, atunci foloseşti bombele. Dar fiecare atac cibernetic american care reuşeşte înseamnă mai puţine avioane şi piloţi americani puşi în pericol. Iar acele bombe inteligente sunt şi ele scumpe, aşadar cyber-războiul poate fi mai ieftin.

TRUPELE CYBER-RĂZBOINICE DIN LUME

Cyber-războiul militar (atacarea computerelor Departamentului Apărării prin internet) nu a provocat încă pagube majore. De partea civililor, costurile pentru a face faţă unui atac cibernetic asupra sistemelor comerciale depăşesc 50 de miliarde de dolari pe an. Încă se mai consideră că cyber-războiul are loc atunci când cineva atacă serios SUA. Adică atunci când unităţile de cyber-războinici îşi dezlănţuie armele cele mai puternice. Încă mai există discuţii între diplomaţi şi avocaţii Departamentului Apărării cu privire la natura războinică a acestor acţiuni. De unde vine această nesiguranţă? Dacă o naţiune poate lansa un atac cibernetic major fără să se legitimeze, cui îi declari război?

Nu este sigur să mergi pe acest drum, pentru că cyber-războinicii americani construiesc în permanenţă arme şi tehnici tot mai bune pentru depistarea originilor atacurilor şi identificarea atacatorilor. Dat tot este posibil

să aibă loc un mare atac anonim, cel puţin teoretic. Nu se ştie dacă o ţară ar risca o astfel de acţiune, pentru că dacă atacul ar avea succes, probabil că SUA ar ignora diplomaţii şi ar declara război oricum. Asta s-a întâmplat cu al-Qaeda şi talibanii, cu toate că niciuna dintre grupări nu îşi asumă responsabilitatea pentru atacurile din 11 septembrie.

Au existat deja unele cyber-războaie de natură legală. În Asia de Est, China şi Taiwan se ceartă de ani de zile pe aceiaşi cyber-războinici. De fapt, au fost tentative de atac serioase, cu toate că ambele părţi neagă acest lucru. Unele acţiuni de hacking asupra site-urilor militare SUA au fost reperate în organizaţiile cyber-războinice chineze.

Pe lângă China şi Taiwan, cele două Corei, Japonia şi Singapore au pus la punct unităţi cyber-războinice. Coreea de Sud a făcut-o pentru a apăra infrastructura electronică a ţării de atacurile venite din partea Coreei de Nord. Timp de mai multe decenii, Coreea de Nord a folosit terorismul, ameninţările şi spionajul pentru a chinui sudul. Liderul Coreei de Nord, Kim Jong Il, este cunoscut ca un utilizator de computer avid, aşa că este uşor să ne închipuim că există un anume entuziasm pentru cyber-război chiar la nivelul conducerii. Coreea de Sud are o populaţie foarte bine pregătită din punct de vedere informatic, iar locuitorii au descoperit că au mult mai multă pregătire pentru cyber-război decât ar fi crezut. Milioane de oameni de aici care au devenit programatori (profesionişti sau amatori) în ultimele trei decenii, pe măsură ce ţara a devenit un important producător de PC-uri şi componente pentru ele, au început să folosească în mod natural internetul şi au descoperit hackingul. Când cei din sud au descoperit ce fel de înşelătorii cyber-războinice pot face nordicii, au început să îşi organizeze apărarea. Din păcate, Nordul are o slabă infrastructură cu care să atace. Dar există China, Rusia şi Japonia. Totuşi, acestea sunt naţiuni cu care China derulează afaceri şi cu care are relaţii destul de bune. Dar Coreea de Sud îşi dă seama că dispune de o armă foarte

puternică. Mai mult decât vecinii ei, cu excepţia Japoniei, Coreea de Sud dispune de oameni foarte talentaţi, care pot duce la bun sfârşit atacuri cibernetice şi, mai important decât atât, pot apăra naţiunea de astfel de atacuri.

Japonia a organizat unităţi cyber-războinice pentru că şi-a dat seama că are cea mai mare expunere electronică în acea parte a lumii, într-adevăr, în vecinătatea Coreei de Nord nu există probabil vreo ţintă cibernetică mai apetisantă decât Japonia. Ambele naţiuni şi-au conectat o foarte mare parte din economie la internet, mai mult decât oricare altă naţiune. Japonezii s-au concentrat pe apărare. Au multe de protejat, dar din motive culturale (sunt foarte politicoşi) şi din cauza agitaţiei persistente cu privire la rolul lor agresiv în cel de al Doilea Război Mondial, nu au făcut prea multe pentru dezvoltarea metodelor de apărare.

Nu la fel se întâmplă cu chinezii, unde există o combinaţie între utilizarea tot mai mare a internetului, extinderea rapidă a industriilor tehnologice şi un puternic simţ naţionalist, care a creat o mare putere cyber-războinică. De asemenea, chinezii sunt unici pentru că guvernul lor a încercat şi a reuşit în mare parte să controleze internetul din China. Desigur, nicio naţiune nu poate deţine controlul absolut asupra internetului. Dar guvernul chinez a mers mai departe decât oricine altcineva. Efortul este susţinut de miile de chinezi capabili, patrioţi şi buni cunoscători ai internetului, care sunt nerăbdători să ajute guvernul în acest sens. Aceşti hackeri chinezi proguvernamentali îi întrec numeric pe acei hackeri black hat independenţi care bagă spaima în guvernele şi companiile din alte ţări.

Oricât de buni ar fi hackerii chinezi, nu au fost în stare să îşi acopere urmele. Unele dintre eforturile lor de peste ocean au fost identificate. Ştim ce pot face chinezii, cel puţin în general, şi ştim că sunt buni. Ce nu ştim este cât de buni sunt şi ce cyber-arme ar putea dezlănţui mai

exact în timpul sau în perspectiva unui război. Acesta este cel mai înspăimântător aspect al războiului cibernetic. Cele mai bune arme sunt acelea care sunt ţinute secrete până la folosire. Victima lovită de un nou tip de cyber-atac trebuie mai întâi să îşi dea seama ce se petrece după care să treacă în apărare şi să remedieze pagubele. Cu cât este mai mare şi mai eficientă forţa cibernetică a unui popor, cu atât pot fi dezvoltate mai multe atacuri neaşteptate şi instrumente.

Exemple despre dibăcia cyber-războiului chinez au fost văzute în luptele duse pe internet între hackerii chinezi şi cei taiwanezi în ultimii ani. Disputa dintre cele două ţări cu privire la independenţa Taiwanului s-a dus în cea mai mare parte pe internet. Acţiunile au fost minore în general, de ştergere reciprocă a site-urilor. Dar au existat indicii că se poate şi mai rău. Cele mai distrugătoare atacuri pe internet au nevoie de multă pregătire, lucru care de obicei presupune să te furişezi în computerele victimei pentru a vedea ce fel de apărare are. În 2000, cyber-războiul dintre cele două ţări a devenit un fel de sport naţional. Dar aceasta a fost doar partea vizibilă a luptei.

Programatorii de ambele părţi au dezvoltat nişte tehnici excelente de apărare a paginilor web, drept urmare a acestor atacuri. Mai puţin evidente sunt încercările regulate de a sparge site-urile militare şi guvernamentale. În august 1999, mai mult de o mie de ATM-uri din Taiwan au fost deconectate din *cauza* unui atac al hackerilor chinezi. Atât guvernul chinez, cât şi cel taiwanez sunt împotriva acestor atacuri, dar neoficial (şi uneori chiar pe faţă) le încurajează. Niciunul dintre „hackerii patrioţi” nu a fost arestat, cu toate că mulţi dintre ei au fost interogaţi de oficialii securităţii propriului guvern. Poliţia secretă a Chinei a supravegheat cu atenţie o parte dintre aceşti hackeri despre care se ştie că dau mai departe informaţii despre punctele slabe ale guvernului. Deşi sute de cyber-

războinici chinezi sunt înrolaţi în armată sau în guvern, există mii de voluntari care sunt oameni liberi la fel ca majoritatea celor de pe internet. Aceşti voluntari a căror identitate este de multe ori necunoscută sunt cei care neliniştesc guvernul. Dar birocraţii comunişti care conduc China sunt dispuşi să suporte acest lucru atât timp cât voluntarii rămân în mare parte loiali guvernului şi sunt capabili să ajute la eforturile cyber-războinice.

La începutul anului 2001, Taiwan a dezvăluit că măreşte forţele secrete ale războiului informaţional la dimensiunea unui batalion. Unităţii i-a fost oferit echipament nou (PC-uri şi instrumente software de ultimă generaţie) şi un cec în alb pentru achiziţiile necesare viitoare. De asemenea a făcut ceva zarvă, lăudându-se cu peste o mie de viruşi gata să fie lansaţi asupra Chinei în cazul unui război. Dacă nu sunt setaţi să atace doar ţinte specifice, aceşti viruşi se răspândesc peste tot pe internet producând mutilări la nivel mondial. În timpul anului 2001, se presupune că Taiwanul a lansat asupra Chinei trei viruşi, care au cauzat aproximativ jumătate din atacurile cibernetice la nivel global. Taiwan are buzele pecetluite atunci când i se cer informaţii despre astfel de chestiuni. Cu toate acestea, nici China nu dezvăluie nimic despre capacităţile ei de atac şi vorbeşte numai despre unităţile defensive. Eforturile ambelor ţări amintesc de faptul că armele cyber-războinice au viaţă scurtă, întrucât depind de erorile de software care sunt în permanenţă descoperite şi corectate. Dar China deţine supremaţia în acest domeniu, căci numărul inginerilor de software şi al hackerilor este în creştere, astfel încât poate descoperi şi exploata erorile de pe internet mai repede decât oricine altcineva.

Partea cea mai proastă este că această ţară nu a ţinut ascuns faptul că susţine acest tip de abordare mai ieftină a războiului. Deşi trebuie plătite salariile (unele foarte mici după standardele SUA) cyber-războinicilor chinezi care lucrează în instituţiile centrale, cea mai mare parte din

muncă este făcută de voluntari patrioţi din rândul inginerilor şi programatorilor chinezi. Avântul acestora a putut fi văzut în altercaţiile cu Taiwan, când voluntarii au intervenit imediat pentru a-şi apăra ţara. Singura parte bună în toată această situaţie este că taiwanezii sunt perfect conştienţi de poziţia lor în liniile fruntaşe ale cyber-războiului ce se pregăteşte. Dar în cazul în care China ar da drumul armelor sale, prima care va suferi va fi Asia de Est, după care haosul va lovi SUA. Conştiente de atacurile-surpriză pe internet pe care le-ar putea lansa China, în anul 2000, forţele aeriene americane au deschis Centrul de Operaţiuni Aerospaţiale din Langley, Virginia. Singura sa misiune era să caute şi să găsească cea mai recentă tehnologie civilă de internet care să confere forţelor aeriene un avantaj în cazul unor atacuri. Una dintre problemele majore ale faptului că armata duce un război informaţional este că, spre deosebire de organizaţiile civile, armata are nevoie de mult mai mult timp pentru a achiziţiona echipamentul certificat pentru uz militar şi a-l distribui trupelor.

Întrucât civilii şi trupele au aceleaşi „arme” într-un război informaţional, armata trebuie să se asigure că nu este scoasă din luptă de populaţia pe care se presupune că trebuie să o apere. În anii ’90 a fost de remarcat viteza cu care chinezii au putut furniza trupelor cele mai noi echipamente pentru computere din producţia civilă, iar SUA încearcă să facă acelaşi lucru, recunoscând că partea chineză are un echipament cyber-războinic mai performant decât cel american. Acest lucru se datorează în mare parte faptului că forţele aeriene cumpără computere, la fel ca oriunde în armată, o dată la câţiva ani. În acea perioadă, livrarea acestora a fost întârziată de procesele intentate de producători, care avuseseră pierderi în urma înţelegerii de a furniza tehnologie nouă. Cum procesele s-au întins pe mai multe luni de zile, tot mai multe persoane din forţele aeriene au remarcat că echipamentele pe care şi le-au

cumpărat pentru acasă sunt mult mai performante decât cele ale guvernului, pe care le foloseau la serviciu. În prezent, forţele aeriene şi-au schimbat politica de achiziţie a PC-urilor, astfel încât să nu rămână în urma potenţialilor duşmani care cumpără aparatură de ultimă oră.

În anul 2000, forţele aeriene americane au creat cea de-a 527-a divizie de atacuri spaţiale. Această unitate avea să fie un partener real pentru cyber-războinicii americani. Acest tip de abordare luase naştere în urma jocurilor de război de la sfârşitul anilor ’90, care au arătat că SUA devin tot mai dependente pe vreme de război de tot mai marea flotă de comunicaţii şi sateliţi de recunoaştere şi navigare. Cu toate acestea, nimeni nu se obosise să caute metode de a ataca reţeaua de sateliţi americani şi atunci când a fost abordată problema s-au descoperit foarte multe vulnerabilităţi. Una dintre cele mai problematice se referea la reţelele de radio care controlau sateliţii. Cu toate că era codat, acest sistem era la fel de vulnerabil ca şi internetul. Şi o mare parte din traficul de pe internet, mai ales cel utilizat de armată, depindea de acei sateliţi pentru a transfera date dintr-o parte a lumii într-alta. Una dintre cele patru subunităţi ale celei de a 527-a divizii s-a specializat în „Red Attack” (descoperirea celor mai eficiente metode de atacare a inamicului, de preferinţă înaintea acestuia). Era deja ceva obişnuit pentru firmele de securizare a internetului să înfiinţeze „Echipe Tiger” de hackeri experţi, care să testeze apărarea organizaţiilor tocmai prin atacarea lor. Echipajul „Red Attack” al forţelor aeriene făcea acelaşi lucru cu reţelele wireless care controlau sateliţii militari ai Americii.

SUA are de asemenea sute de cyber-războinici în cadrul FBI unde sunt vânaţi hackerii implicaţi în acte criminale. Dar nu numai FBI şi Departamentul Apărării sunt în căutarea numărului tot mai mare de criminali cibernetici. Trezoreria americană este responsabilă de depistarea falsurilor, a spălărilor de bani şi de orice alt tip

de fraude financiare. În anul 2000, a adoptat în cele din urmă religia internetului şi a cerut ca Serviciile Secrete să fie extinse cu o sută de agenţi care să fie antrenaţi în arta crimei pe internet.

Multe dintre instrumentele de hacking folosite de infractori sunt similare, de multe ori identice cu acelea folosite de cyber-războinici, astfel că pe timp de război FBI şi Trezoreria americană vor avea şi ele resurse cyber-războinice.

MISTERIOASA CHINĂ ÎŞI DEPĂŞEŞTE TRECUTUL

La sfârşitul anului 2001, China a sărbătorit prima generaţie de ofiţeri care au urmat un curs de un an despre operaţiunile psihologice pe timp de război. Ţara organizase deja mai multe unităţi cyber-războinice şi investea foarte mulţi bani în antrenamentul inginerilor experţi. Un factor major de motivaţie pentru acest program este conştientizarea faptului că internetul şi mass-media au devenit arme militare puternice. Există o mare ironie aici deoarece, pentru mai multe mii de ani, China s-a aflat în primul front a dezvoltării noilor operaţiuni de război psihologic. Interesul chinezilor faţă de această formă de război a făcut ţara să pară atât de exotică pentru străini. De exemplu, se ştie că în China medievală se folosea foarte mult practica luării ostaticilor, ceva ce nu era necunoscut nici în Europa. Regele cerea ca principalii nobili (sau potenţiali trădători) să îşi trimită unul dintre fii la curtea sa. Motivul oficial pentru asta era ca tânărul fiu (de multe ori un copil de opt-nouă ani) să îl poată cunoaşte pe rege şi viceversa. Motivul adevărat era că dacă tatăl băiatului l-ar fi trădat pe rege, „ostaticul” ar fi fost ucis. În ceea ce priveşte loialitatea, chinezii erau foarte practici, după cum se vede. De exemplu, o zicală chineză spunea: „Cea mai uşoară cale de a cuceri o fortăreaţă este cu un măgar”. Adică un măgar încărcat cu aur şi argint pentru mituirea

garnizoanei. De aceea familiile celor mai mulţi dintre comandanţii de fortăreţe locuiau în altă parte, într-un loc unde oamenii împăratului să nu îi poată ucide atât de repede, dacă tăticul vindea fortăreaţa împăratului.

Pe scurt, chinezii au conştientizat de multă vreme importanţa reţelelor de informaţii, a încrederii (în generalii şi comandanţii principalelor fortăreţe) şi a instrumentelor pentru influenţarea amândurora şi pentru conducerea guvernului.

Plini de ingeniozitate, înţelepţii chinezi au scris multe cărţi despre cum să foloseşti trucurile războiului psihologic şi informaţional pentru a-l face pe comandantul fortăreţei să se predea necondiţionat. Cum? Simplu: întocmeşte un raport fals care să ajungă la împărat şi care să spună că fortăreaţa a fost vândută pe mită. Apoi te asiguri că cel care comandă fortăreaţa a aflat despre moartea soţiei şi a copiilor (câteodată, alături de bunici, fraţi sau surori). Dacă reuşeşti să faci asta (nu e uşor dar s-a întâmplat de multe ori) probabil vei obţine fortăreaţa la jumătate de preţ, pentru că acel comandant va fi furios că i-a fost ucisă familia. Mesajele false, zvonurile bine plasate şi alte tehnici dorea să deţină mai mult control asupra criptării, ceva ce oamenii care dirijau şi utilizau internetul doreau ca nimeni să nu aibă. FBI doreşte să poată pătrunde oriunde pe internet (cel puţin în Statele Unite) şi să poată citi orice material codat trimis sau primit de firmele americane. Deşi declară că încearcă doar să apere pe toată lumea de infractorii internetului, cei mai mulţi utilizatori de internet (atât indivizi, cât şi companii) îl văd ca pe „fratele mai mare”.

FBI avea totuşi o piaţă pentru software-ul lui, şi anume agenţiile guvernamentale. Sistemul Intra Guard era un software creat pentru a apăra reţelele (guvernamentale sau private) de atacurile cibernetice. Opţiunile lui includeau detectarea activităţii suspecte şi înregistrarea datelor pentru investigaţiile ulterioare. Intra Guard era

practic un produs comercial aprobat de FBI. Astfel era mai uşor de vândut agenţiilor guvernamentale, dar clientela tradiţională a FBI era împotriva vânzărilor către organizaţii nonguvernamentale. Iar companiile nu doreau ca FBI să monitorizeze ce fac ele pe internet.

Existau şi probleme de cooperare. Această problemă a existat întotdeauna între FBI şi alte agenţii guvernamentale. FBI vrea să culeagă informaţii, dar nu doreşte să ofere nimic. Este o problemă veche. Multe agenţii au învăţat să se descurce cu acest obicei prost al FBI. Totuşi, în acest caz, celelalte agenţii, mai ales CIA şi Departamentul Apărării, au simţit că sunt mai bine echipate pentru a face faţă problemelor de securitate pe internet şi şi-au dat seama că se pot lipsi cu totul de

FBI. Mai mult, NIPC nu poate merge pe urmele infracţiunilor de peste ocean, ăsta este terenul CIA. în plus, atacurile pe internet pot fi uşor făcute să pară că provin de peste ocean, iar cele din afara SUA pot fi făcute să pară că provin din America de Nord. Din fericire, acest tip de înşelătorie a devenit mai uşor de descoperit. Dar până să aibă cei de la NIPC habar de unde vine atacul, se diminuează posibilitatea ca FBI să preia cazul sau nu.

În 2000, pentru a face lucrurile mai interesante, Departamentul Apărării a încercat să preia controlul asupra operaţiunilor de război informaţional prin reorganizarea bugetului militar, astfel încât să includă o organizaţie separată care să facă ceea ce făcea deja NIPC. FBI s-a împotrivit, iar NIPC a câştigat. Dar când George Bush a devenit preşedinte în 2001, Departamentul Apărării a făcut din nou o mişcare pentru a conduce războinicii informaţionali. Problema era încă sub semnul întrebării la începutul anului 2002 şi va continua probabil să rămână aşa, întrucât birocraţii se luptă între ei pentru controlul asupra noului câmp de luptă şi asupra tuturor banilor adiţionali care sunt investiţi în războiul informaţional.

De asemenea, la început, cea mai mare parte din

resursele NIPC erau folosite pentru instruirea agenţilor FBI în legătură cu investigaţiile misterioase de pe internet sau pentru a susţine investigaţiile FBI. Deşi FBI a declarat că era unul din apărătorii securităţii internetului, celelalte agenţii guvernamentale nu s-au împăcat cu ideea. FBI era ignorat şi se luau măsuri pentru preluarea rolului

„Conducerii” în securitatea internetului de către Departamentul Apărării. FBI-ului nu i-a surâs deloc ideea şi, începând de la 11 septembrie 2001, a arătat un mai mare grad de cooperare şi bun-simţ. Fără îndoială, un rol în această nouă atitudine l-a avut un raport critic al Biroului Guvernamental de Audit din iulie 2001. Cam în aceeaşi perioadă, propriii tehnicieni ai NIPC au reuşit să infesteze reţeaua internă cu virusul Sirlam. Era extrem de jenant, întrucât cine mai avea încredere în FBI pentru a-l proteja de problemele de pe internet dacă nici măcar nu se poate apăra singur de un virus obişnuit?

Firmele de securitate pe internet erau foarte descurajate de lipsa de cooperare a FBI. Acesta punea multe întrebări, dar dădea puţine răspunsuri. Nu era tocmai un schimb liber de informaţii. Mai mult, FBI ŞI NIPC erau depăşite de potenţialul hackerilor existenţi în firme. Puteai crede că FBI nu spune multe pentru că nu prea are multe de spus. Acest lucru părea confirmat de faptul că aproape toate alertele de securitate ale NIPC erau pentru atacuri care erau deja în plină desfăşurare. De fapt, NIPC luase fiinţă într-o lume în care organizaţiile, în mod special CERT şi alţi câţiva furnizori de software antivirus, creau deja alerte. De asemenea, CERT avea o relaţie mult mai bună cu firme şi cu agenţiile guvernamentale.

O altă problemă era că cei mai mulţi hackeri black hat care puteau fi prinşi tindeau să fie ori minori americani ori străini din ţări unde hackingul nu era pedepsit prin lege. Cele mai multe companii erau reticente cu privire la abilitatea FBI de a prinde hackeri. De aceea, numai

aproximativ o treime dintre atacurile hackerilor sunt raportate. Lumea afacerilor şi-a dat seama de multă vreme că de fapt guvernul nu are resursele necesare pentru a investiga intruziunile sau pentru a preda vinovatul, în cazul în care îl prind, FBI-ului – care să îl aresteze şi să îl judece. FBI nu vrea să recunoască faptul că primeşte astfel de cazuri care i se înmânează după ce partea cea mai grea din investigaţie a fost făcută deja. Firmele implicate sunt de multe ori mulţumite să se conformeze numai să rămână în termeni buni cu federalii.

Performanţele lipsite de strălucire din jurul NIPC ŞI FBI sunt măcar recunoscute la Washington ca fiind o problemă. Dar, momentan, nimeni nu are o soluţie.

CYBER-RĂZBOINICII DISPĂRUŢI

Forţele armate americane au îmbrăţişat internetul şi odată cu el pericolul de a fi atacate pe această cale. Dar luând în calcul cât de vulnerabile pot fi trupele, instituţiile au de-a face cu o tot mai evidentă dispariţie a experţilor de care au nevoie pentru a se apăra.

Aceşti „soldaţi” cu experienţă în calculatoare pleacă în turmă. Un motiv ar fi oportunităţile mai bune din punct de vedere economic de pe piaţa civilă. Dar un alt motiv esenţial este volumul extrem de mare de muncă ce este pus pe umerii acestor cyber-războinici. Pe măsură ce forţele armate instalează tot mai multe reţele, întâmpină mai multe probleme şi o mai mare expunere la hacking. Problema principală este că cea mai bună apărare împotriva spargerii reţelelor sunt administratorii de sistem, care să actualizeze şi să securizeze software-ul. Cele mai multe spargeri sunt urmare a unui software prost instalat sau neactualizat cu ultimele îmbunătăţiri şi protecţii. Cererea de administratori de sistem bine pregătiţi îi face pe tinerii militari cu astfel de abilităţi să fie la mare căutare pe piaţa civilă. Armata a avut ceva de furcă pentru a-i convinge să se reînscrie.

Un alt motiv important care îi face pe cyber-războinici să nu rămână înrolaţi prea mult este obligaţia de a transloca aceste trupe atunci când apare o nouă situaţie de criză. Armata foloseşte peste tot reţele şi lucrează la echiparea infanteriei de luptă şi a vehiculelor blindate cu astfel de reţele. Când trupele sunt trimise în locuri precum Bosnia, sunt setate reţele locale (şi conectate peste tot în lume cu sateliţii mobili). Au existat probleme cu acest lucru în Bosnia; ca urmare, mulţi cyber-războinici s-au trezit trimişi din nou acolo, de mai multe ori. Problemele cu reţelele şi computerele din alte zone oarecum mai liniştite precum Coreea, Afganistan şi Golful Persic creează o altă cerere de specialişti care să fie trimişi acolo. Nu este modul de viaţă ideal pentru cei mai mulţi oameni, mai ales pentru soldaţii căsătoriţi.

Iar astăzi majoritatea soldaţilor sunt căsătoriţi. De multe ori trupele trebuie să aleagă între cariera militară şi căsnicie. De obicei câştigă cea din urmă.

Atunci când internetul s-a răspândit la începutul anilor ’90, armata lucra deja la „interconectarea” navelor, avioanelor şi tancurilor. Astfel puteau fi trimise informaţii despre ţinte şi date, despre locul unde se aflau forţele aliate şi cele inamice. Uşurinţa cu care putea fi folosit internetul părea o soluţie ideală. Dar exista şi un revers al medaliei. Internetul era creat de mii de programatori independenţi. Software-ul era de multe ori gratuit şi actualizat în permanenţă de voluntari pasionaţi. Atunci când modifici foarte mult un software, mai faci şi greşeli. Greşelile care îţi scapă sunt cele care nu afectează operaţiunea, ci mai degrabă compromit securitatea. Aceste capcane şi fisuri sunt cauza celor mai multe atacuri. Cealaltă mare gaură în securitate este munca din interior, adică o parolă furată. În cazul sistemelor guvernamentale, aproximativ 95% din intrările ilegale în sistem sunt acte de spionaj care implică de obicei o parolă furată. Cea mai bună apărare împotriva acestor probleme sunt

administratorii de reţea competenţi care încearcă să controleze toate modificările de software şi să îşi actualizeze sistemele. Dar niciodată nu au fost suficient de mulţi administratori de reţea, iar atunci când armata şi-a extins reţelele a descoperit că duce lipsă de cyber-războinici. Angajarea contractorilor civili mult mai scumpi, de multe ori foşti cyber-războinici, ajută într-o oarecare măsură. Dar Congresului nu îi place preţul mult mai mare pe care îl percep civilii.

Armata încearcă să se adapteze folosind tot mai multă automatizare pentru actualizarea software-urilor. Corporaţiile, care se confruntă cu aceeaşi lipsă de personal, merg şi ele în aceeaşi direcţie. Dar pentru repararea sistemelor automate sunt utili în mai mare măsură civilii. Acest lucru face diferenţa. Aşadar armata încearcă să compenseze prin restricţionarea severă a gradului în care serverele militare pot fi setate şi accesate. Deşi această politică este frustrantă pentru trupe, oferă totuşi o mai bună securitate. Dar asta nu compensează faptul că armata nu reuşeşte să păstreze personalul tehnic calificat, în caz de cyber-război, această criză de personal va fi responsabilă pentru eventualele înfrângeri.

ECHIPA DE EVALUARE A RISCULUI ONLINE

Recunoscând că personalul său pentru securitate web nu se ridică la nivelul experţilor civili, Departamentul Apărării a apelat la vechea tehnică de a aduna rezerviştii cu abilităţile speciale de care era nevoie şi le-a dat mână liberă. La începutul anului 2000, Departamentul Apărării a instituit o unitate de rezervă plină de experţi în internet care avea să petreacă un weekend pe lună verificând site-urile militare publice cu informaţii delicate sau clasificate (care nu aveau ce căuta acolo). Această unitate, cunoscută sub numele Web Assessment Team (sau WRAT, aşa cum îşi spunea unitatea) este un exemplu tipic pentru noua abordare a Departamentului Apărării în ceea ce priveşte

securitatea computerelor. După ce a parcurs 800 de site-uri web care aveau legătură cu Departamentul Apărării, echipa a găsit 1.300 de subpagini cu probleme de securitate. Au fost găsite zece site-uri unde erau postate detalii despre planurile de război (de obicei strict secrete) ale Statelor Unite. WRAT este de asemenea responsabil pentru îmbunătăţirea securităţii site-urilor acestei instituţii şi foloseşte o serie de tehnici demonstrate (dezvoltate de companiile comerciale în apărarea propriilor secrete) pentru a face asta.

CYBER-REZERVIŞTII

Înainte ca Statele Unite să aibă o armată, aveau rezervişti locali. În mare parte, era o chestiune legată de bani. Soldaţii cu normă întreagă sunt scumpi. Ideea rezerviştilor, care de fapt este una antică, foloseşte pur şi simplu civili antrenaţi şi echipaţi pentru a se lupta ca o armată. Atunci când există o ameninţare, sunt chemaţi rezerviştii.

Ei bine, încă ne mai aflăm în epoca rezerviştilor, atunci când vine vorba de trupe care pot purta un cyber-război. Singura problemă este că nimeni nu i-a organizat pe aceşti rezervişti. Cu excepţia WRAT (descrisă mai sus), ideea este doar o altă propunere ce dă târcoale Pentagonului.

Propunerile în sine variază. Una dintre ele a avut ca rezultat înfiinţarea WRAT. Altele au identificat hackeri talentaţi printre oamenii care activau deja în rezervele unităţilor de război secret şi electronic. O altă propunere este formarea unei forţe speciale de securitate pentru supravegherea internetului. Problema principală a unei forţe de poliţie cu normă întreagă este că momentan (şi în viitorul apropiat) există o atât de mare lipsă de forţă de muncă (instruită, ca să nu mai spun talentată) încât ar fi dificil să organizezi o astfel de unitate cu nivelul de salarizare al guvernului.

O soluţie ar fi încercarea de a organiza şi recompensa eforturile *pro bono* care se depun de ceva vreme pentru securitatea cibernetică. Mulţi hackeri white hat talentaţi se satură şi pleacă singuri în căutarea tipilor răi. Un astfel de exemplu este proiectul Honey Net (reţeaua voluntară a serverelor Honey Pot7 creată pentru a atrage, analiza şi raporta activităţile şi tehnicile folosite de hackerii black hat).

Armata a instituit deja unităţi de rezervă cyber-războinice, pentru că armata a avut deja peste un milion de oameni în unităţi de rezervă. Câteva mii dintre aceştia sunt calificaţi ca experţi în internet, în cea mai mare parte datorită slujbelor lor civile. Mulţi alţii ar putea fi aduşi la acest nivel cu instruire suplimentară. Acest tip de instruire ar putea fi oferită de guvern şi foarte puţini ar refuza, pentru că i-ar putea ajuta să avanseze în carierele actuale.

La fel ca multe gărzi naţionale şi unităţi în rezervă, companiile cyber-războinice şi batalioanele pot fi chemate în caz de urgenţă naţională, în acest caz, nu ar fi pentru uragane sau incendii forestiere, ci pentru situaţii în care există un avânt al vandalismului pe internet sau chiar un cyber-război. La începutul anului 2001, a existat un asemenea eveniment, când hackerii Chinei au atacat infrastructura internetului american din cauza incidentului cu avionul EP-3. Mai târziu în acelaşi an, rezerviştii cu expertize internet au fost chemaţi să ajute din nou la războiul împotriva terorismului. Singurul dezavantaj al acestor unităţi este că mulţi membri au slujbe în domenii legate de internet, slujbe unde li se simte lipsa atunci când sunt chemaţi în cazul unei urgenţe. Dar angajatorii lor ştiu acest lucru şi îşi pot reorganiza activitatea.

O altă opţiune pentru guvern ar fi să înfiinţeze o cyber-corporaţie ca o companie controlată de guvern, să găsească oameni foarte bine pregătiţi, să le dea foarte mulţi bani şi mână liberă. Cyber-corporaţia ar putea să plătească la nivelul pieţei oamenii potriviţi şi să aibă în

acelaşi timp o bună relaţie cu agenţiile guvernamentale şi firmele care cheltuiesc foarte mult pentru securitatea reţelelor (bănci şi firme de intermediere, de exemplu). Fiind o corporaţie separată, cu scopuri bine definite, cyber-corporaţia nu ar fi întinată de operaţiunile politicilor de birou cărora le-a căzut pradă NIPC. Cea mai mare parte din activitatea infracţională de succes e rezultat al neglijenţei victimei. În privinţa aceasta cyber-corporaţia nu ar putea face prea multe. Dar majoritatea înşelătoriilor de pe internet ar putea fi eliminate dacă acesta ar fi suficient de bun pentru a vâna şi strânge informaţii despre ce fac vandalii black hat. Aceşti ţipi nu fură atât de mult pe cât distrug. Dar pentru o companie care trebuie să plătească milioane de dolari pentru costuri de personal suplimentar care să repare pagubele, nu este o situaţie cu mult diferită de un furt pe faţă. FBI ar putea face arestări în continuare şi nu ar trebui să îşi mai facă griji pentru a atrage hackeri extrem de talentaţi cu un nivel scăzut al salarizării.

Soluţia tradiţională pentru acest tip de problemă este încheierea unui număr mare de contracte cu „Beltway Bandits” (firmele de consultanţă în domeniul apărării din zona Washington, DC). Asta este ceea ce au făcut Forţele Speciale Armate în 2000. Au fost identificate 14 proiecte, dintre care majoritatea se ocupau cu cercetarea unor modalităţi mai bune pentru a apăra computerele de hackeri. Intenţiile erau foarte bune. Guvernul dorea să dezvolte un software care să urmărească activitatea din interiorul serverului şi să activeze o alarmă dacă vreun utilizator părea a fi un hacker ce încearcă să preia controlul asupra serverului. Celălalt mare domeniu de cercetare era dezvoltarea unui software care nu numai că declanşa o alarmă şi aştepta intervenţia umană, dar ar fi oprit automat unele părţi din sistem pentru a împiedica orice activitate din partea hackerului. În mod sigur erau nişte măsuri care meritau efortul. Dar existau câteva probleme legate de modul în care Departamentul Apărării

avea de gând să procedeze. În primul rând, deşi consultanţii în apărare aveau oameni excelenţi, nu erau la fel de buni ca cei din industria securităţii internetului, deoarece un software precum acesta este dezvoltat întotdeauna de piaţa civilă. Dar Pentagonul putea controla acei Beltway Bandits în moduri în care nu putea controla firmele comerciale. Există o relaţie amiabilă între Departamentul Apărării şi aceşti consultanţi. Dacă Pentagonul are nevoie de un studiu care să arate că ratarea înregistrată a fost de fapt o mişcare sclipitoare, există un consultant în apărare care poate realiza asta. Aceşti oameni fac foarte multă muncă utilă, dar pentru că supravieţuirea lor depinde de numărul de contracte încheiate, actele necurate de genul acesta sunt doar un preţ mic de plătit pentru a face afaceri. Pentagonul a avut succes în a încheia contracte cu cercetători universitari sau consultanţi care să cerceteze zonele exotice. Aşa a fost pornit şi internetul. Dar într-un mediu care se dezvoltă rapid din punct de vedere tehnologic, studiile sunt deja învechite înainte să fie terminate. Structura şi atmosfera liberă a internetului sunt foarte populare printre cei din noua generaţie de hackeri. Nu poţi schimba acest lucru, iar dacă armata şi guvernul nu vor face rost de forţa de muncă de care au nevoie, exceptând situaţia unui război major şi mobilizarea naţională, va fi nevoie de nişte idei inovatoare de recrutare şi organizare.

CUM VA ARĂTA CYBER-RĂZBOIUL

De fapt, foarte puţine atacuri pe internet vor omorî oameni în mod direct. Cu toate acestea, nu asta este ceea ce îi îngrijorează pe cei din armată. Pentru că în prezent internetul este centrul unei reţele mult mai mari, forţele armate pot fi mai puţin eficiente dacă internetul este atacat cu succes. Asta înseamnă că mai multe trupe americane ar fi ucise în vreme ce pagubele inamicului ar fi mai mici. De exemplu:

Mesajele false de e-mail pot fi uşor trimise. Şi copiii pot face asta şi uneori chiar o fac. O serie de mesaje false sau derizorii trimise de cineva care are o listă de ordine şi recunoaşte cum trebuie să arate un mesaj legal, poate provoca foarte multe pagube înainte să ne dăm seama. Dacă îţi baţi capul să verifici toate textele de neînţeles care însoţesc mesajele de e-mail şi ştii ce trebuie să cauţi, poţi să îţi dai seama foarte repede cum arată un mesaj fals. Dar înainte să îşi dea seama cineva că mesajele nu sunt reale, mii de astfel de texte vor fi dat peste cap activitatea forţelor noastre, trimiţând nave, avioane, provizii, sateliţi şi unităţi terestre în direcţii greşite. S-ar crea haos pentru mai multe zile, dacă nu chiar săptămâni, în plus, inamicul (care a trimis mesajele false) ar şti unde se îndreaptă oamenii tăi, putându-şi îmbunătăţi posibilităţile de atac. Toate astea pot fi făcute de inamic prin simpla infiltrare în reţelele noastre pe timp de pace. Exact acest tip de lucruri se petrece acum. Problema este că nimeni nu a inventat încă instrumentele necesare prinderii tuturor pungaşilor sau măcar detectării lor. Şi noi procedăm la fel.

— Un alt atac pe internet în primele faze ale unui război ar fi unul care corupe bazele de date militare. De fapt, nu ai vrea să corupi (amestecarea aleatorie a datelor) aceste baze de date în modul tradiţional, întrucât ar fi emis un mesaj de eroare atunci când trupele şi strategii noştri le-ar folosi. Nu, trebuie să faci schimbări care să asigure trimiterea greşită a proviziilor şi a pieselor de schimb de către sistemele automate de reaprovizionare. Vrei să schimbi ţintele bazelor de date, astfel încât proiectilele şi bombele noastre inteligente să rateze ţinta, iar echipamentul nostru electronic să detecteze şi să bruieze mai greu radarele inamice. Programele de „adormit” sunt un software care este implantat într-un computer de pe o navă de război. Când aceste programe sunt activate, computerele şi *bazele* de date ale navei pot fi paralizate în nenumărate moduri. Poţi de asemenea implanta programe

de „adormit” în computerele forţelor aeriene sau unităţilor armatei. Activarea lor se face printr-o comandă trimisă pe internet sau atunci când computerul victimei face anumite lucruri precum rularea programelor ce indică punerea la cale a unui război. Implantarea acestor programe este cea care ocupă timpul unităţilor pe timp de pace (şi căutarea lor). Este greu să le implantezi, dar nu imposibil. Şi atunci când găseşti unul dintre aceste programe, e de preferat să îl ţii secret. La fel ca o capcană camuflată controlată printr-o telecomandă, vrei să dezactivezi programele de „adormit”, dar să faci inamicul să creadă că sunt încă intacte şi gata de a fi folosite.

— Înşelătoria pe internet poate scoate din uz unele echipamente. Echipamentele militare sunt numite, pe bună dreptate, „de înaltă performanţă”. Asta înseamnă că pot funcţiona în siguranţă, în cea mai mare parte a timpului, în limitele performanţelor pe care le au. Înseamnă că un asemenea dispozitiv este mai rezistent la eşecuri în cazul în care este distrusă o componentă importantă. Operatorii echipamentelor militare (avioane, arme, electronice) sunt instruiţi cu grijă astfel încât să ştie când utilizează aceste echipamente peste limita lor. Această situaţie nesigură este permisă în cazul armatei pentru că în luptă ai de multe ori de ales între a fi ucis cu siguranţă sau a fi probabil ucis dacă forţezi limitele acestor aparate. Cele mai bune exemple sunt avioanele cu reacţie. În vreme de război, piloţii pot forţa motoarele şi o parte din componentele electronice un pic mai mult. Asta înseamnă că motorul poate fi distrus cât de curând, dar viteza mai mare pe care o ai îţi poate salva viaţa în luptă.

Astăzi, o mare parte dintre aceste echipamente riscante sunt controlate total sau parţial de software. O altă îmbunătăţire este că poţi modifica uşor acest software pentru a face echipamentul mai eficient împotriva noilor tehnici descoperite de inamici. Uneori aceste schimbări sunt făcute printr-o reţea, de cele mai multe ori sunt

făcute pe un computer conectat le reţea, după care software-ul nou este manual adus la echipament şi descărcat. Astfel poţi vedea ce fel de posibilităţi are cineva care ştie câte ceva despre software-ul tău şi a obţinut acces la reţelele tale.

— Există un anumit tip de program de „adormit” numit „adulmecător”. Acest program va copia mesajele şi datele transmise de tine şi le va trimite direct la tipii răi. Poate de asemenea analiza mesajele şi datele trimise. În cazul în care identifică ceva foarte important, adulmecătorul va pândi transmisia. Dacă nu opreşti toate mesajele care corespund profilului, vei provoca pagube şi utilizatorului îi va fi mai greu să îşi dea seama că are un software inamic pe computer. Din când în când oamenii se aşteaptă ca ceva să nu mai meargă bine la computerul lor. Aşa că, atât timp cât utilizatorul caută o eroare şi nu un adulmecător, poţi continua să produci pagube pentru mai multă vreme.

— Toate aceste pagube nu trebuie neapărat să fie îndreptate numai către ţinte militare. Pentru a însemna ceva, atacurile trimise coalizat trebuie să fie îndreptate către ţinte mai mari, care să se prăbuşească sau care să ne afecteze serios capacitatea de a ne apăra. Sunt anumite ţinte specifice către care şi-ar îndrepta inamicul atacurile cibernetice. Dacă trimiţi atacurile individuale către zone prea diferite, pagubele totale vor fi mai puţin răsunătoare. Vrei să provoci foarte multe pagube într-o clasă de ţinte, pentru a avea un efect decisiv. Există trei tipuri de arii de atac asupra cărora e bine să te concentrezi:

Deplasarea forţelor. Aici sunt incluse nave, trupe de luptă terestre şi avioane care sunt trimise într-o zonă de război. Dacă ele pot fi încetinite sau scoase din funcţiune, chiar şi numai pentru o vreme, asta va afecta lupta. Toate unităţile de luptă americane depind de accesul la internet în timp de pace şi, într-o mai mică măsură, în timpul operaţiunilor de război. Fiecare navă are propria reţea de

internet, dar şi alte reţele. Navele de război şi cele de întărire sunt cele mai vulnerabile în faţa atacurilor pe internet. Unităţile forţelor aeriene îşi petrec mai mult timp cu partea de logistică (se ocupă de provizii) şi întreţinerea avioanelor de război care se îndreaptă spre luptă. Poate că cele mai vulnerabile ţinte ale forţelor aeriene, cel puţin în forţele aeriene americane, sunt sutele de transporturi. Avioanele de război nu se pot lupta peste ocean fără un avion care să transporte piese de schimb, arme şi alte provizii şi care să-l însoţească. Un atac major concentrat asupra unităţilor aeriene de transport ar da peste cap deplasarea forţelor americane peste ocean. De asemenea, ar întârzia deplasarea unei divizii aeriene.

Facilităţi critice. Armata foloseşte noţiunea „misiune critică” pentru a se referi la ceva care, dacă eşuează, ar putea periclita succesul operaţiunii. În capul listei s-ar afla orice are legătură cu transporturile sau comunicaţiile. Aeroporturile militare şi civile sunt foarte puternic dependente de computere şi reţele. Un atac cibernetic asupra lor le-ar putea opri pentru mai multe zile sau le-ar reduce capacităţile pentru o perioadă mai lungă decât atât. Centrele controlate prin satelit sunt şi ele vulnerabile. Aici pagubele ar putea fi şi mai mari. Dacă atacul cibernetic ar fi suficient de puternic, ar putea scoate de pe orbită mai mulţi sateliţi. Ca să le poţi înlocui ai avea nevoie de luni sau chiar ani de zile. Alte facilităţi vulnerabile în cazul unui atac sunt centralele de energie nucleară, cele de energie electrică şi sistemul telefonic. Lovirea puternică a oricăreia dintre ele ar avea efecte militare demne de luat în seamă. Sistemele minciunilor critice. Aici ne referim la computere sau grupuri de computere specifice, care controlează o anumită funcţiune militară. Deşi Departamentul Apărării are mii de reţele diferite de calculatoare, o mică parte dintre ele sunt considerate „critice”. Desigur, acestea sunt cel mai bine protejate sisteme şi cel mai greu de spart, ceea ce face ca un atac

cibernetic asupra lor să fie şi mai util. Exemple de astfel de sisteme sunt acelea care controlează traseul proviziilor, accesul la sateliţi spioni, transporturile aeriene şi navale (ce transportă, unde se află şi încotro se îndreaptă), detalii despre războiul electronic, structura reţelelor de comunicaţii şi aşa mai departe. Înţelegi la ce mă refer. Unele sisteme de computere guvernamentale pot duce de asemenea la implicaţii dacă sunt dezactivate, precum acelea care se ocupă de plătirea firmelor ce furnizează materialele militare (de la bocanci la bombe). Departamentul de Justiţie este în permanenţă pus în gardă cu privire la spioni şi sabotori. Dacă inamicul poate pătrunde în computerele

Departamentului de Justiţie care conţin informaţii despre ce crede SUA cu privire la spionii străini, pot fi provocate foarte multe pagube.

Internetul s-a dovedit a fi extrem de util pentru armată, dar în acelaşi timp, aceasta a căpătat o foarte mare vulnerabilitate. Militarilor le este mult mai uşor să acceseze internetul şi să beneficieze de avantajele lui decât le este să construiască apărarea împotriva atacului cibernetic. SIPRNET (versiunea codată a internetului, care nu este conectată la internetul obişnuit), deşi este mult mai sigur, este de asemenea mult mai puţin util decât internetul obişnuit.

Nu vom şti cine a câştigat cursa pentru utilizarea internetului ca armă militară până când nu va izbucni un război şi vom afla cine este mai vulnerabil şi cine are cele mai puternice arme. Cyber-războinicii lumii se pregătesc pentru acest război şi sunt pe bună dreptate neliniştiţi cu privire la cine va câştiga, atunci când acel război va izbucni.

CAPITOLUL 9
ARMELE ŞI INSTRUMENTELE CYBER-RĂZBOINICULUI

TERMENI TEHNICI

Glosarul complet, ce include şi termenii definiţi mai jos, poate fi găsit la sfârşitul cărţii.

Decriptarea înseamnă spargerea codurilor (chei de criptare) folosite pentru a păstra informaţiile secrete. Înaintea secolului XX, se referea la descifrarea puzzle-urilor, întrucât pe vremea aceea criptarea se baza pe lucruri precum substituirea (folosirea anumitor numere sau simboluri în locul literelor). Dar în ultima sută de ani, au fost create aparate care să utilizeze coduri mai complexe, iar în timpul celui de-al Doilea Război Mondial au fost create computere care să testeze mai rapid toate „substituirile" posibile pentru spargerea codurilor. Practic, decriptarea se referă fie la folosirea unor computere mai puternice pentru a încerca toate combinaţiile posibile până poţi citi codul, fie la (şi asta îi sperie cel mai mult pe utilizatorii de criptare) folosirea unor algoritmi speciali pentru a găsi erori în rutina de substituire.

Exploatarea datelor se referă la o nouă tehnologie în care sunt folosite cantităţi imense de date, precum achiziţionarea de produse de către milioane de indivizi anual, ca instrument statistic de găsire a unor corelaţii utile. De exemplu, ce fel de produse cumpără oamenii înaintea sau în timpul anumitor evenimente (plecarea în vacanţă, în preajma sărbătorilor) pentru diferite niveluri de venit. Exploatarea datelor dezvăluie tipare de cumpărături necunoscute înainte şi favorizează o mai bună comercializare. Această abordare există de mai bine de un secol, dar, folosind exploatarea datelor, beneficiul este mult mai rapid şi mai exact.

Instrument pentru ghicirea parolei – este un

program (numit de multe ori şi „dicţionar de parole”) care foloseşte o listă extinsă (uneori cu peste un milion de elemente) a parolelor cunoscute sau tipice pentru a putea intra ilegal pe un site sau pe un server protejat prin parolă. Nu ai nevoie decât de un nume de utilizator. Aceste instrumente nu mai sunt la fel de utile cum erau, pentru că tot mai multe site-uri blochează numele de utilizator pentru care se introduc prea multe parole incorecte (între trei şi zece, de exemplu) una după alta. Apoi site-ul îi spune utilizatorului să încerce din nou peste aproximativ cinci minute. Este în regulă pentru un utilizator adevărat şi suficient de mult pentru a face programul de ghicire a parolei ineficient. În acest fel, ar dura zile întregi să testezi sute de mii de parole posibile. Fără acea suspendare, instrumentul de ghicire ar da rezultate în câteva minute sau în cel mult o oră.

Armata, mai ales cea din Statele Unite, a preluat internetul repede şi cu aplomb. Pentru că războiul nu este tipul de context la care ne gândim atunci când ne referim la internet, trupele au avut nevoie de ceva imaginaţie pentru a face lucrurile să meargă. Armata americană a învăţat cum să utilizeze internetul ca armă de luptă în cea mai mare parte a anilor ’90. După toată această perioadă, încep să apară o mulţime de arme militare „eficientizate de internet”.

Un aspect neobişnuit al creării de instrumente militare pentru internet este că cele mai multe au fost elaborate iniţial de civili. Aşa că trupele au trebuit să adapteze o mare parte din instrumentele de hacking civile pentru utilizare militară.

CUTIA CU UNELTE A CYBER-RĂZBOINICULUI

Din punctul de vedere al cyber-războinicului, cea mai bună parte a muncii sale este că armele sunt ieftine şi uşor de obţinut. De fapt, nu trebuie să cari nimic după tine. Toate armele esenţiale sunt disponibile pe internet sau pot

fi înmagazinate acolo. În acelaşi timp, unii cyber-războinici pot să îşi depoziteze cutia cu unelte pe propriul tău computer.

Mai mult, poţi antrena un cyber-războinic în numai câteva săptămâni. Cele mai multe dintre instrumentele de bază pot fi găsite pe internet ca echipament pentru orice PC conectat la internet. Mii de soldaţi cyber-războinici pot fi instruiţi cu uşurinţă într-o perioadă scurtă de timp. Teama ne este provocată de faptul că e un lucru pe care l-ar putea face şi o ţară precum China. Deşi mulţi hackeri experimentaţi îşi vor automatiza o mare parte din muncă, sunt încă unele lucruri care funcţionează mai bine dacă este implicată şi un pic de judecată umană. Hackerii sub acoperire nu au fost niciodată prea bine ascunşi. Intră pe internet, mergi la un motor de căutare (precum google.com) şi scrie „hacker tools” (cu ghilimele). Vei obţine peste 10.000 de rezultate. Ceea ce se află pe prima pagină accesată este mai mult decât suficient pentru oricine.

Cei care creează instrumentele de hacking o fac destul de natural pentru a fi cât mai uşor de utilizat. De ce să le pui la dispoziţia tuturor? În mare parte pentru că singura recompensă pentru cei mai mulţi hackeri este propria mândrie. Sunt mândri atunci când creează cele mai eficiente instrumente. Exista o vreme, cu un foarte mulţi ani în urmă, când hackerii se lăudau cu ce reuşeau să facă datorită acelor instrumente. Dar acest lucru este mai puţin întâlnit azi. Federalii sunt mai vigilenţi şi sunt destul de buni la identificarea oricărei persoane care vorbeşte mult prea mult despre spărturile provocate. De asemenea există o mai mare probabilitate ca poliţia să îi trimită la închisoare pe hackeri, mai degrabă decât să le dea o amendă sau să ceară o pedeapsă cu suspendare. Dar mai este un motiv pentru care există atât de multe astfel de instrumente. Cei care protejează internetul le folosesc pentru a fi siguri că serverele lor sunt în siguranţă.

Folosind instrumente de hacking, mai ales pe acelea care examinează milioanele de computere conectate la internet, căutând terminale neprotejate care le vor permite să recurgă la alte înşelătorii, poţi măcar să vezi cu ce te confrunţi.

Instrumentele de bază sunt Verificatorii de securitate, Scanerele de reţele şi Adulmecătorii de pachete. Acestea sunt folosite pentru a găsi serverele vulnerabile sau chiar PC-urile conectate la internet. Dacă ai de gând să spargi un sistem, primul lucru pe care trebuie să îl faci este să găseşti unul în care poţi intra. Scanerele sunt de obicei automatizate şi setate să verifice, raportând situaţiile în care găsesc sisteme vulnerabile. Această abordare automatizată poate iniţia un program de verificare, deşi acest lucru este mai eficient atunci când este făcut cu supravegherea unui om. Un astfel de program pătrunde mai adânc într-un sistem vulnerabil obţinând mai multe detalii despre cum este setat şi despre gradul de vulnerabilitate. Adulmecătorii de pachete pur şi simplu preiau datele care intră sau ies dintr-un sistem pentru a încerca să obţină parole sau pur şi simplu pentru a supraveghea informaţiile necodate care se află acolo. Sunt mii de programe care fac aceste verificări, scanări sau adulmecări. De asemenea, vei găsi instrumente şi sfaturi pentru combaterea acestora. De aceea este nevoie de atât de multă activitate pentru crearea acestor instrumente. Are loc un război şi nimeni nu reuşeşte să aibă decât o victorie de moment. Aşa că în fiecare zi sunt create noi căi de apărare şi atac. La sfârşitul anilor ’90, puteai verifica şi scana fără teamă, pentru că nu erau multe site-uri care să se ferească de aceste activităţi. Nu mai este cazul. Oamenii sunt prinşi în efracţie, iar numărul condamnărilor, sau cel puţin al depistărilor, este tot mai mare. Aşadar trebuie să înveţi şi cum să îţi ascunzi urmele. Acest lucru se întâmplă în cazul cyber-războinicilor, deşi nu toate forţele militare sunt atât de precaute pe cât ar

trebui. Un număr tot mai mare de intruziuni şi spargeri sunt identificate ca venind din locuri suspecte precum Rusia sau China. Vorbim despre iniţiative ale unor instituţii controlate de guvern, nu numai despre universităţile din cele două ţări.

Testarea şi scanarea fac parte din instructajul de bază al noilor cyber-războinici. Spargerea unui site vulnerabil necesită foarte multă îndemânare şi experienţă. Marea diferenţă dintre miile de încercări de hacking care au loc în fiecare zi şi cyber-război este că majoritatea încercărilor de a pătrunde în computerul altcuiva sunt făcute de amatori. Astfel de lucruri sunt un fel de hobby pentru foarte mulţi copii şi destul de mulţi adulţi. Cyber-războinicii care sunt antrenaţi pentru a lansa atacuri militare pe internet operează diferit, chiar dacă instrumentele folosite sunt similare cu cele utilizate în fiecare zi de script kiddies sau de hackeri profesionişti.

Kitul de instrumente pentru hackerii militari va fi mai standardizat, pentru că orice operaţiune militară pentru cyber-război va implica sute sau chiar mii de oameni. Instrumentele standardizate fac mai uşoară instruirea oamenilor şi compararea rezultatelor între cei care fac parte din echipă. De asemenea, uşurează actualizarea instrumentelor tuturor, ceea ce trebuie făcut frecvent. Internetul este într-o permanentă schimbare şi asta înseamnă că şi instrumentele de care este nevoie pentru a fi spart trebuie să se schimbe. În plus, creatorii acestor instrumente găsesc mereu metode tot mai bune pentru a le exploata.

Un alt lucru de ţinut minte. Detalii despre cum operează mai exact cyber-războinicii este un secret extrem de bine păstrat. Un lucru înţeles foarte repede de cei implicaţi în această formă de război a fost că secretizarea este cea mai puternică armă din arsenalul tău cibernetic. Cu cât inamicul ştie mai multe despre cum operezi, cu atât mai puţin succes vei avea. Aşadar, ceea ce descriu este

cum ar trebui să se organizeze şi să opereze orice organizaţie cyber-războinică. S-au scurs destul de multe informaţii în ultimii ani, pentru a ne da de înţeles că mai sunt multe de aflat.

Chiar dacă sunt obţinute informaţii despre o reţea a inamicului (printr-un spion sau un e-mail trădător – orice ar fi ia-l cu tine), tot trebuie să scanezi şi să verifici pentru a confirma că este informaţie reală şi nu vreo capcană.

Scanarea şi verificarea sunt părţile cele mai uşoare în dezvoltarea unui atac cibernetic. Toată desfăşurarea pentru pregătirea unui atac poate fi rezumată printr-un acronim: SPAA (Scanează, Probează, Analizează, Atacă). De multe ori mai sunt şi alţi paşi de urmat dacă vânezi un site ce nu este disponibil publicului. Un exemplu ar fi reţelele private de internet ale armatei (SIPRNET, Intelink, NIPRNET ŞI GOVNET). Numai obţinerea accesului la aceste reţele este o operaţiune majoră şi ar ţine mai mult de tehnicile tradiţionale de spionaj şi ascultare a convorbirilor. În timpul Războiului Rece, SUA au folosit un submarin nuclear pentru a intra în sistemul secret de comunicaţii militare al Rusiei. Asta pentru că o parte a cablului transoceanic de comunicaţii traversează o bază de submarine ruseşti de pe o insulă. Acea realizare a fost mai târziu demascată de un trădător american şi acelaşi tip de înşelătorii au loc şi în cazul cyber-războiului. Este o afacere murdară.

Cyber-războinicii ar lăsa pe seama altora (spioni, agenţi străini, trădători) obţinerea accesului la reţelele private, lucru necesar pentru a provoca pagube serioase ţintelor militare. Dar o mare parte dintre ele sunt conectate la internetul la care avem cu toţii acces. Iar aici şi-ar depune eforturile şi ar pune în aplicare instrumentele majoritatea cyber-războinicilor.

INSTRUMENTE ŞI TEHNICI ALE METODEI SPAA (SCANEAZĂ, PROBEAZĂ, ANALIZEAZĂ, ATACĂ)

Scanarea poate fi descrisă cel mai bine ca fiind schiţarea (şi actualizarea) unor hărţi ale unui internet mereu în schimbare. Acestea nu sunt hărţi adevărate, în cele mai multe cazuri, ci liste uriaşe cu locaţii de pe internet şi cu ce se află acolo mai exact (din punct de vedere tehnic). O mare parte dintre acestea sunt făcute cu instrumente disponibile, majoritatea fiind automatizate. Pur şi simplu dai drumul acestor scanere peste tot sau măcar într-o secţiune din internet şi primeşti înapoi raporturi cu ce au găsit. Internetul este o bestie uriaşă cu peste 50 de milioane de servere şi peste două miliarde de pagini web. Practic, scanarea înseamnă cartografierea unei anumite porţiuni din internet, dar pentru scopurile militare americane este nevoie de o actualizare constantă a hărţii întregului internet, cu mai multe detalii despre zonele militare şi guvernamentale. „Harta” este stocată într-o bază de date, iar această bază de date este un bun de mare importanţă al armatei. Este de asemenea şi un instrument major pentru cyber-războinicii tăi şi o parte dintre uneltele noi-nouţe ar trebui adoptate pentru a putea lucra cu această bază de date. Scanarea pe internet se face la un nivel foarte ridicat şi se bazează pe detectorii de scanere puşi pe o serie de servere. Dacă stai pe internet mai mult de câteva ore, probabil vei fi scanat. Dacă pui un server nou pe internet, în numai câteva ore va începe să fie scanat. Multor oameni le place să facă hărţi ale internetului. De fapt, mare parte din această scanare provine din dorinţe pur mercantile (precum comercializarea hărţilor de internet sau verificarea automată de actualizări pentru software-ul PC-ului). Dar, de asemenea, este făcută de script kiddies sau alte persoane ce caută să înşele. Cyber-războinicul doreşte să identifice serverele militare sau guvernamentale şi să vadă cât de bună este securitatea lor. În unele cazuri, anumite tipuri de organizaţii militare/guvernamentale au automat parte de mai multă atenţie după ce au fost identificate în

timpul unei scanări. Altfel, numai site-urile care sunt foarte vulnerabile sunt vizitate din nou pentru a fi folosite pentru atacuri. Scanarea profită de faptul că fiecare computer de pe internet trebuie să poată furniza automat anumite informaţii tehnice, atunci când sunt cerute de un alt computer. Aceste întrebări şi răspunsuri automate ţin de acele rutine ale internetului care menţin webul în funcţiune. Dar un hacker foloseşte acest sistem de identificare periodică pentru a obţine multe informaţii utile referitor la cine îl foloseşte şi ce structură are.

Probarea este un tip de scanare mai detaliată, în care hackerul va înşela sistemul automat (în moduri prea tehnice pentru a fi explicate aici) pentru a obţine mai multe informaţii despre structura unui server sau a unei reţele locale. Dată fiind creşterea măsurilor de securitate de pe internet, probarea înseamnă o mai bună examinare a unui server. Uneori acest lucru este făcut cu un instrument automat. Adesea, ţinta studiată este ea însăşi o reţea conectată la internet. Dacă scanările şi probările tale vor găsi un site cu adevărat valoros, vei trimite un hacker talentat pentru a-l verifica şi nu vei folosi un sistem automat. Atunci când testezi trebuie să ai grijă să nu fii detectat. Este mai puţin probabil ca un hacker uman să facă ceva care să declanşeze alarma de intruziune, spre deosebire de unul automat. Începând cu anul 2000, utilizarea detectării intruziunilor de software a devenit ceva obişnuit. Acest software a fost creat pentru a prinde hackerii în mijlocul acţiunii, fără a le da de ştire că sunt urmăriţi. Administratorul serverului ar fi astfel anunţat şi ar începe un joc de-a şoarecele şi pisica, în care hackerul are rolul şoarecelui.

Toată această activitate ar fi înregistrată într-un jurnal pentru analize ulterioare. Normal, cei mai competenţi hackeri sunt de obicei destul de dibaci pentru a recunoaşte un detector de intruziune pe server şi evită să fie descoperiţi. Întotdeauna este posibil să treci de un

astfel de detector, aşa cum este posibil să treci de majoritatea sistemelor de alarmă ale clădirilor. Mai întâi afli ce fel de sistem de detecţie este folosit (există tot felul de indicii, dar unele dintre ele sunt foarte vagi şi subtile). Dacă eşti destul de bun pentru a-ţi da seama cu ce fel de sistem de detecţie te confrunţi, profiţi de slăbiciunile lui şi reuşeşti să treci de el. Nu este la fel de simplu pe cât ne este prezentat în filme. Şi aici are avantaj armata cibernetică cu cel mai vast kit de instrumente. Mai mult, experţii în securitate şi cyber-războinicii americani deţin supremaţia, pentru că cea mai mare parte din software-ul internetului este creat în Statele Unite. Astfel americanii au un acces mai bun la secretele acestuia. Dacă nu se profită de un asemenea avantaj (prin folosirea lui, ignoranţa poate fi un element decisiv în cazul unui cyber-război. Dar uneori un truc vechi precum „alarme false frecvente" poate face un administrator de sistem enervat să dezactiveze sistemul de detecţie. Acest procedeu a fost folosit foarte multă vreme de tâlharii profesionişti pentru a trece de sistemele de *alarmă,* (cei de la pază se satură să tot descopere că nu are loc niciun jaf, se decid că e ceva în neregulă cu alarma şi o opresc pentru restul nopţii până va fi verificată de tehnician dimineaţa). A fost folosit şi pentru atacarea serverelor bine protejate. Un administrator de sistem bine pregătit va recunoaşte trucul, dar nu toţi sunt atât de ascuţiţi la minte.

Uneori, trebuie însă să rişti atunci când probezi, mai ales atunci când, de exemplu, pare că programul tău de ghicire a parolei ţi-ar putea obţine accesul ca utilizator „legal". Spre deosebire de alte instrumente şi arme cyber-războinice, care sunt ţinute secrete până la izbucnirea războiului, instrumentele de test trebuie folosite pe timp de pace, când toţi cei implicaţi adună constant informaţii despre cum funcţionează adversarul. De asemenea, se pot obţine informaţii despre modul de operare al trupelor cibernetice ale fiecărei naţiuni.

Poate dura mult timp să analizezi site-urile şi reţelele inamicului. Ce încercăm să aflăm este modul în care este gestionat site-ul şi ce hardware şi software este utilizat pentru asta. Există mii de programe diferite şi componente de calculator care pot fi folosite într-un server şi toate combinaţiile vor avea un rezultat diferit dacă încerci să intri prin efracţie. Dacă obţii un acces total (capacitatea de a rula oricare dintre programele site-ului), munca ta este mult mai uşoară. Dar cu site-urile bine protejate de azi, analiza ta trebuie să testeze noi combinaţii. Trebuie să te furişezi, în cazul în care reuşeşti să intri şi chiar să aduni informaţii din bârfele de pe net, presa publică sau alte site-uri. De fapt, în cazul site-urilor cu adevărat importante se fac analizări în mod constant. Asta pentru că serverele care ţin site-urile în funcţiune sunt în permanenţă actualizate. Ceea ce înseamnă că site-ul pe care l-ai probat şi analizat atât de amănunţit luna trecută va fi un site cu totul diferit peste câteva luni. Şi asta înseamnă că atacul tău bazat pe analizele precedente va fi mai puţin eficient.

De fapt, atacul asupra site-urilor are loc în două faze. Pentru site-urile pe care ai putut să pătrunzi, poţi lăsa în urmă câteva bucăţi de software utile pentru monitorizarea site-ului şi raportarea celor aflate. Dar există riscul ca acele bucăţi de software să fie descoperite. Aşa că trebuie să pui în balanţă riscurile şi beneficiile. În cazul atacurilor DDOS (Distributed Denial of Service) ai nevoie de programe care să transmită multe „deşeuri” serverului pe care vrei să îl dezactivezi. Cele mai bune locuri pentru a le implanta sunt PC-urile care sunt mereu conectate la internet prin conexiuni de mare viteză. Asta înseamnă computere personale cu modem prin cablu sau conexiuni DSL. în cazul site-urilor la care vrei să îţi păstrezi accesul, mai ales pe vreme de război, e indicat să pui un program foarte bine camuflat care să observe ce se petrece şi, desigur, să păstreze accesul activ. Este un lucru extrem de valoros, întrucât îţi permite nu numai să aduni parole, dar

şi să depăşeşti problema site-urilor care îşi schimbă constant parolele. Este însă greu să faci asta, pentru ca cele mai multe dintre site-urile importante sunt mereu scanate şi analizate de proprietarii care caută exact astfel de programe inamice. Dar chiar şi dacă nu laşi nimic în urmă, analizarea site-urilor-ţinta îţi oferă o imagine mai bună despre armele care le-ar putea doborî într-un moment crucial. Aceste „încărcături de război" sunt programe trimise către site-urile sparte chiar înainte de a izbucni războiul. Uneori, ele vor face acelaşi lucru ca programele plus alte sarcini imediate precum coruperea sau distrugerea datelor. Există şi viruşi care pot fi eliberaţi ca parte a unui atac cibernetic. Aceşti viruşi sunt creaţi pentru a şterge site-urile inamice, şi nu pe ale tale sau cele ale prietenilor şi aliaţilor tăi. Există cantităţi imense de instrumente disponibile pe web pentru crearea viruşilor şi o mare parte din cyber-războinicii oricărei ţări îşi vor petrece majoritatea timpului creând sau modificând viruşi. Majoritatea naţiunilor cu un program cyber-războinic activ au arsenaluri de zeci sau sute de astfel de viruşi speciali pentru război.

Aceste naţiuni cu forţe cibernetice, adică majoritatea ţărilor, trebuie de asemenea să îşi apere luturile de instrumente şi arsenalul. Deşi acesta din urmă (conţinând viruşi şi alte încărcături războinice) este stocat pe reţele ce nu sunt conectate la internet, trupele cibernetice trebuie să fie online în cea mai mare parte a timpului, cu propria scanare, probare şi analizare a instrumentelor. Ori de câte ori nu sunt, pot fi observate şi analizate. Gândeşte-te la ele ca la un mare joc de şah, dar unul în care îţi poţi crea singur piesele şi poţi modifica regulile.

SIPRNET ŞI AMENINŢAREA

În 1994, exact la timp pentru explozia utilizării internetului datorită apariţiei Word Wide Web,

Departamentul Apărării a înfiinţat SIPRNET. Era o reţea care folosea tehnologia şi instrumentele internetului, dar funcţiona complet separat de acel internet. SIPRNET a fost construit pentru a transmite mesaje şi documente strict secrete. În acelaşi timp, guvernul a creat INTELINK (un internet separat, pentru ca FBI, CIA, DEA, ASN să facă schimb de informaţii) şi NIPRNET (un alt internet distinct, neclasificat, pentru armată). SIPRNET era de asemenea criptat (toate datele erau trimise folosind un cod secret) şi considerat a fi invulnerabil. Sau nu? La sfârşitul anului 1999, nişte experţi în reţele de la Departamentul Apărării au devenit un pic îngrijoraţi. Agenţia pentru Siguranţa Naţională şi alte organizaţii au creat „echipe Red" de hackeri pentru a ataca reţelele Departamentului Apărării cu instrumente de hacking disponibile pe scară largă. Normal, în unele locuri au intrat şi în altele nu. Dar cel mai înfricoşător lucru învăţat a fost că sistemele Departamentului Apărării nici măcar nu au detectat 99% dintre atentate (reuşite sau nu).

Acest lucru i-a pus pe oameni pe gânduri în legătură cu cât de sigur este SIPRNET. Cei din interior ştiau că este, teoretic, posibil să spargi SIPRNET. Dar credeau că ar fi fost nevoie de resurse considerabile sau de ajutor din interior. Pe măsură ce erau prinşi tot mai mulţi spioni după Războiul Rece şi era conştientizat faptul că unii dintre ei s-ar putea să nu fie prinşi niciodată, perspectiva unui om din interior care să ajute la spargerea SIPRNET a devenit o posibilitate. Colapsul Uniunii Sovietice din 1991 a trimis mulţi (acum şomeri) maeştri sovietici în spionaj către SUA ca să îşi caute de lucru. Aceşti ţipi au fost mult mai eficienţi decât am crezut şi nimeni nu mai poate presupune acum că este puţin probabilă pentru ei o slujbă în interior. La sfârşitul anilor '90 s-a aflat că sovieticii au cumpărat, mituit şi şantajat atât de mulţi oameni care lucrau în guvernul american, încât existau foarte puţine mari secrete pe care sovieticii să nu le aibă.

Departamentul Apărării trecuse deja prin nişte experienţe jenante cu viruşi care, într-un fel sau altul, intrau de pe internet pe reţele protejate (sunt mai multe, dar SIPRNET este cea mai bine păzită şi singura reţea strict secretă). De obicei, povestea e aceeaşi, utilizatorii iau un virus de pe internet, îl mută pe computerul SIPRNET printr-o dischetă şi se răspândeşte. Un alt mod, deşi mai puţin frecvent, este atunci când un server care este conectat la internet este mutat fizic într-o nouă clădire, unde cineva spune: „Hei, avem nevoie de un alt server pentru lucrurile de pe SIPRNET şi este unul nefolosit aici…" Firesc.

„Noul" server a adunat probabil ceva viruşi atunci când a fost conectat la internet, care se răspândesc în tot SIPRNET-ul.

Se presupune că ambele tipuri de probleme ar fi trebuit rezolvate până acum, dar o altă problemă cu SIPRNET este că totul în legătură cu el este atât de secret încât numai câteva persoane sunt autorizate să îi verifice securitatea. Şi mai există şi posibilitatea mereu actuală a unui om din interior care să trădeze SIPRNET-ul. În lumea reală, este de mult timp recunoscut faptul că sursa principală a intruziunilor serioase (în comparaţie cu cele de amuzament) este un om din interior care furnizează parolele şi alte informaţii importante, de care este nevoie pentru a intra într-un sistem atât de bine protejat.

Odată ce problema Y2K a fost rezolvată, Departamentul Apărării a început să cheltuiască miliarde de dolari pentru a întări securitatea şi reţelele. Aici era inclus *şi* SIPRNET, care a avut parte de acelaşi tip de supraveghere constantă pe care o primeau reţelele neclasificate. Acest efort a fost considerat necesar pentru ca SIPRNET (care a folosit mereu propria reţea de legătură prin satelit, linii terestre şi cabluri subacvatice) să ofere acces tot mai multor locaţii din lume.

„Succesul" SIPRNET-ului a dus la nevoia creării

GOVNET-ului, un internet separat pentru întreg guvernul. De fapt, este o idee bună, dar nu din motivele pe care şi le închipuie cei mai mulţi oameni. Cele mai mari probleme ale internetului nu sunt numărul de ciudaţi şi nebuni care trimit viruşi. Nu, marile probleme sunt anom mitatea şi capacitatea de a-ţi proiecta liber propriul spaţiu web atunci când ai nevoie. GOVNET, care nu se află în spaţiul public, ar face ca fiecare utilizator să fie responsabil. Nimeni nu ar fi anonim. Nu ar exista instrumente vitale pentru hackeri, disponibile pe GOVNET care ar fi, practic, proprietatea guvernului. Singurul software disponibil aici ar fi lucrurile de care este nevoie pentru afacerile guvernului. Cealaltă cauză a insecurităţii internetului sunt software-urile prost scrise, care ar putea fi controlate pe GOVNET. Pe site-urile acestuia nu ar avea voie să funcţioneze decât software aprobat. Poate că nu va fi la fel de sclipitor ca site-urile comerciale, dar va fi mai sigur. Ce vrei mai mult de la guvern? Dacă vrei lumini, mergi la Hollywood!

De fapt, guvernul nu este prea încântat de GOVNET. În primul rând instalarea lui costă miliarde de dolari şi dă mai mult de muncă angajaţilor. Cum va fi un spaţiu cibernetic paralel, nu vei putea accesa aceleaşi site-uri ca pe internet. Desigur, fiecare birou guvernamental va avea unul sau mai multe PC-uri conectate la internetul obişnuit. Dar un motiv nerostit pentru reticenţa faţă de GOVNET este incapacitatea de a schimba reţeaua, pentru activităţi nelegate de slujbă. Şi acele câteva aparate conectate la internet vor fi probabil într-o zonă comună pentru mai mulţi angajaţi unde nu vei putea naviga de plăcere fără a fi observat. Mai mult, motivul principal pentru care fiecare birou guvernamental va avea o conexiune obişnuită la internet este acela că guvernul va păstra unele site-uri ca serviciu public şi vor trebui gestionate e-mailurile primite de la cetăţeni şi organizaţii nonguvernamentale, care nu au acces la GOVNET. Poţi avea PC-uri setate să acceseze şi

GOVNET-ul şi internetul, dar asta înseamnă că viruşii luaţi de pe internet vor ajunge în acelaşi computer care se conectează la GOVNET. Există modalităţi prin care poţi preveni mutarea viruşilor de pe o reţea pe alta, cel puţin teoretic. Dar practic, nu vor avea efect 100%, şi nici măcar 50%.

Avem deja un exemplu în acest sens cu INTELINK (internetul izolat, pentru organizaţiile ce dispun de informaţii secrete din SUA), care pur şi simplu nu a fost folosit prea mult. Până după 11 septembrie 2001, când toată lumea implicată în serviciile secrete s-a adaptat şi a început să folosească INTELINK, pentru o vreme. Dar aşa cum a demonstrat internetul, dacă creezi ceva ce atrage natura umană, oamenii vor veni. Procedează invers pentru a împiedica oamenii să meargă în tot felul de locuri ciudate, şi vor sta la depărtare. Internetul privat ţine la distanţă nebunii şi hackerii, dar nu este atrăgător nici pentru utilizatori.

Mai este şi problema banilor. Guvernul SUA cheltuieşte aproape 50 de miliarde de dolari pe an pentru computerele şi reţelele lui. Jumătate sunt pentru Departamentul Apărării şi majoritatea afacerilor strict secrete sunt încredinţate reţelelor acestui departament. Urgenţa de a mări securitatea chestiunilor foarte critice (strict secrete) este mai mare decât cea a protejării agenţiilor guvernamentale, ale căror site-uri pot fi atacate de viruşi şi hackeri cu intenţii rele, fără a fi ucişi oameni.

EXPLOATAREA DATELOR, OLAP ŞI PERIEREA

Acest ocean tot mai mare de documente electronice oferă o şansă unică de război informaţional, precum exploatarea datelor. Aceasta a fost inventată pentru a ajuta departamentele de marketing în vânzarea produselor. Ideea din spatele exploatării datelor este destul de simplă. Folosind computere şi programe de statistică, poţi săpa prin cantităţi imense de date în căutarea unor corelaţii

utile între grupurile de oameni (mai ales cei înstăriţi) şi anumite produse. Profesioniştii în marketing caută să cumpere şi să producă tipare preferenţiale, astfel încât să poată fi dezvoltate produse noi de succes, iar cele deja existente să poată fi îmbunătăţite. Cine cumpără aşa ceva? Sau, mai important decât asta, cine vrea să cumpere ceva ce nu există încă? Producătorii şi vânzătorii au adunat îndelung date despre preferinţele clienţilor, dar „exploatarea" manuală a acestor date nu a fost întotdeauna profitabilă. Cu ajutorul computerului este.

Exploatarea datelor comerciale a ajuns la maturitate în anii '90, când computerele s-au ieftinit şi au devenit suficient de puternice pentru a face faţa masei de date colectate de vânzători şi producători. Exploatarea tradiţională a datelor aplica doar instrumentele obişnuite de statistică pentru corelarea unor categorii diferite de date. Dar această abordare s-a schimbat în anii '90, atunci când noile software-uri şi PC-urile mai puternice au permis comercianţilor şi nu numai, statisticienilor sau altor maniaci să facă aceste analize.

Comercianţii nu erau prea interesaţi de modul în care se făceau acestea, atât timp cât puteau extrage unele informaţii utile cu care să facă bani. Odată ce oamenii au început să câştige bani din exploatarea datelor, au fost investite sume mari în sistemele de exploatare a datelor, iar statisticienii şi programatorii au devenit mai interesaţi. Acest lucru a dus la ideea de procesare analitică online (OLAP1, cunoscut *şi* sub numele de Analiză Rapidă a Informaţiilor Multidimensionale împărţite sau FASMI2). Pe Wall Street, OLAP este realizata cu o masă constantă de date despre piaţa financiară, dar ceea ce a făcut-o specială este faptul că OLAP are caracteristicile unui joc video. Utilizatorul programului de exploatare a datelor poate pune o întrebare despre cine produce cărămizi sau o altă marfă *şi* obţine informaţiile grafic. Iar graficul poate fi o curbă de distribuţie familiară (puncte mici înşirate în jurul

unei linii care merge din colţul stâng din partea de jos a ecranului înspre colţul drept de sus). Poţi obţine orice imagine vrei (grafice în formă de plăcintă, în formă de bară sau chiar grafice 3D). Toate acestea au dus la noi tehnici şi noi termeni de specialitate. Astfel avem „perierea”, care îi permite utilizatorului să selecteze orice fel de date disponibile şi să şteargă sau să adauge un alt element, în general să caute prin date până găseşte ceea ce caută sau cel puţin ceva util. Această abordare interactivă pentru care nu este nevoie de statisticieni bine pregătiţi sau experţi în computere este foarte populară printre oamenii de afaceri şi analiştii informaţiilor secrete.

Nici firmele din domeniul public şi fără îndoială nici CIA nu vor pierde prea mult timp cu OLAP, dar vor lucra off-line folosind informaţii din băncile de date. Acesta este un alt termen nou şi se referă la terabiţi (mii de gigabiţi) de date ţinute pe hard drivere pentru analize instant. Dar pentru cyber-războmici, OLAP va servi ca unul dintre cele mai puternice instrumente. Nu neapărat o arma, ci mai degrabă un mijloc de căutare, care nu numai că va evidenţia informaţii dar va descrie şi ce se ascunde în spatele aparenţelor. Analiza a milioane de atacuri asupra sistemelor de computere este o muncă tipică pentru OLAP. Din motive practice, ar fi imposibil să treci manual prin toate acele date. Cu OLAP poţi face asta în câteva minute.

Cele mai multe companii folosesc OLAP pe baze de date mari, pentru a afla când şi cine le-a achiziţionat produsele pe parcursul a mai multe luni sau mai mulţi ani. Important e că nu trebuie să fii un expert pentru a folosi software-ul OLAP. Dacă îţi cunoşti afacerea (de exemplu, vânzarea de parfumuri sau motociclete), poţi găsi rapid tipare de vânzare prin folosirea acestui program.

S-a descoperit că exploatarea datelor are de asemenea şi utilizare militară. Agenţiile de informaţii secrete, mai ales de la apariţia sateliţilor-spion şi renaşterii electronice, au colectat mult mai multe

informaţii decât puteau sorta. Este un mic secret murdar al instituţiilor secretizat acela că există depozite pline de casete cu date care nu au fost niciodată examinate. Fotografii făcute prin satelit, semnale electronice şi mesaje, toate au fost adunate în cantităţi mult prea mari pentru a putea fi examinate.

Evident, agenţiile de informaţii secrete au fost primele care au văzut aceste oportunităţi. Utilizarea software-ului ca să sortezi toate aceste lucruri poate duce la aflarea unor informaţii importante despre forţele armate străine; unde se află, cum operează. Nu ai putea niciodată să angajezi, să plăteşti şi să instruieşti suficient de mulţi analişti umani pentru a face asta. Erau pur şi simplu prea multe date, care conţineau prea puţine informaţii utile. Tehnologia pentru exploatarea datelor a schimbat totul. În anul 2000, s-a strecurat informaţia că CIA cerea Congresului o sumă mare de bani cu care să cumpere mai multe computere noi care să examineze, ei bine, tot internetul, permanent, până în cel mai mic detaliu. Inclusiv fiecare chat room (sau măcar o parte dintre ele, pentru că multe sunt protejate de parole, deşi şi acest lucru se poate rezolva). Ca parte a acestui proiect, CIA vrea să construiască o reţea separată bazată pe internet, astfel încât angajaţii CIA să poată face schimb de informaţii în mai multă siguranţă. De asemenea, CIA doreşte să cumpere noi computere şi echipamente de reţea pentru a-şi îmbunătăţi eforturile actuale de a pătrunde în companiile şi organizaţiile suspecte că ar susţine organizaţiile duşmane Statelor Unite.

Nu a fost prima incursiune a CIA în exploatarea datelor. La începutul anilor ’80, a cumpărat foarte multe noi staţii de lucru. Software-ul era creat pentru a permite analiştilor să sape printre gigabiţii de date pe care îi avea agenţia în fişierele existente. Era util, dar să nu uităm că cele mai noi computere de azi sunt de peste o sută de ori mai rapide (şi mult mai ieftine) decât staţiile de lucru de

acum 20 de ani. În ziua de azi, poţi face o exploatare a datelor serioasă şi rapidă. Succesul în vânarea multora dintre teroriştii din anii ’90 s-a datorat în parte acestor eforturi de exploatare a datelor.

Acum CIA vrea să relanseze jocul acesta şi să meargă în căutarea tuturor bulgărilor de aur îngropaţi în miliardele de pagini web, mesaje *Usenet* şi conversaţii din chat room, plus cel mai probabil, o mare parte din traficul e-mailurilor. Este o analiză clasică a informaţiilor dar la o scară nemaiauzită. Cu atât de mulţi oameni pe internet, sunt foarte mulţi cei implicaţi în planuri teroriste ucigaşe care vor lăsa să scape bucăţi mici de informaţii în momente şi locuri diferite. Pentru teroriştii de pe internet, informaţiile pe care le lasă în urmă nu par să aibă vreo valoare secretă. Dar dacă faci rost de suficient de multe astfel de informaţii şi le pui repede cap la cap, poţi afla lucruri utile despre cine ce face, cu cine, cui, când şi cu ce.

Altfel spus, dacă sunt câteva sute de milioane de oameni ce comunică în mod constant pe internet, nu se poate să nu existe şi informaţii utile. Ajută să poţi citi mesajele electronice ale celorlalţi oameni, iar CIA face acest lucru de mai multe zeci de ani. Dar şi mai utilă este abilitatea de a sorta marele râu de date pe care îl reprezintă internetul. Astfel vor ieşi la iveală lucruri a căror existenţă era necunoscută. Din păcate, din cauza naturii secrete a CIA, nu vom afla niciodată ce au făcut mai exact şi cum au procedat, cel puţin nu până când aceste date vor fi declasificate – zeci de ani de aici înainte. Dar ştim, din ce au făcut utilizatorii comerciali cu exploatarea datelor sau din ce plănuiesc să facă, ce poate scoate o agenţie de informaţii secrete de pe internet. Pe scurt, organizaţiile de informaţii secrete pot extrage multe elemente importante din cantităţile imense (miliarde de mesaje) de date. De exemplu, dacă sute de terorişti din jurul lumii menţionează, în termeni vagi şi neoficiali, un anumit tip de operaţiune şi alţii menţionează o anumită

persoană-cheie (folosind chiar nume diferite), toate aceste date pot fi puse cap la cap, ca într-un joc de puzzle mortal. Foarte curând, observi un tipar pentru o anumită operaţiune şi afli cine sunt cei implicaţi în ea.

DISPOZITIVELE DE ASCULTARE ŞI RĂZBOIUL INFORMAŢIONAL

Când au apărut primele sisteme de comunicaţie electronică în anii 1850, nu a trecut mult timp până ca cineva să îşi dea seama cum să asculte (urcai pe un stâlp de telegraf şi ataşai propria cheie de telegraf de cablul acestuia printr-un alt fir). Astfel auzeai ceea ce era bătut de operatorii de telegraf care foloseau linia. Cheia de telegraf era un dispozitiv care arăta ca maşina de scris cu o cheie. Dacă apăsai pe cheie, se întrerupea curentul electric şi se auzea un clinchet la capătul celălalt al firului. Acest tipar al clinchetelor (codul Morse) a început să nu mai fie folosit de armata prin anii ’90.

Dispozitivele de ascultare au fost vreme îndelungată un instrument valoros pentru prinderea criminalilor, spionilor sau teroriştilor. În anul 2000, erau 1.190 de dispozitive aprobate de instanţă în SUA, o parte dintre ele pentru spionaj şi investigaţii de terorism. Numărul lor exact este secret, dar probabil nu depăşeşte câteva zeci. Cele mai multe astfel de dispozitive se foloseau în cazurile cu droguri. FBI îşi dăduse seama deja ca cele mai bune informaţii despre spionaj şi terorism vin de peste ocean şi SUA avea (şi încă mai are) o mare reţea de sateliţi care adună informaţii, staţii la sol şi nave. America are mână liberă pentru a aduna informaţii de peste ocean, dar multe restricţii legale se aplică în SUA. Şi guvernul şi-a dat seama că spionii şi teroriştii profitau de internet. Aşa că la sfârşitul anului 1999, FBI a venit cu ideea de a intercepta traficul de pe internet pentru a căuta mesaje primite sau trimise de terorişti. „Ascultarea” se face prin obţinerea unui ordin judecătoresc pentru un ISP (precum AOL) care

să permită computerelor FBI să verifice toate mesajele ISP care vin sau care pleacă. Această abilitate tehnică a fost numit CARNIVORE. În vara anului 2000, FBI a declarat că acesta este singurul factor important pentru detectarea şi respingerea a până la şase atacuri pe zi ale al-Qaeda (organizaţia lui Osama bin Laden). Această urmărire a internetului nu face decât să caute o listă de cuvinte pe care, să zicem, teroriştii islamici le folosesc în e-mailurile lor. Cauţi mesaje de e-mail care conţin de exemplu cuvinte precum:

„Allah", „distruge", „necredincios" (nonmusulman). Poţi de asemenea căuta mesaje care vin sau se duc la anumite adrese de e-mail şi, pe lângă mesajele care conţin cuvintele suspecte, poţi lua toate mesajele pentru o analiză ulterioară. Dacă mesajul este codat, trebuie să decizi dacă merită efortul de a-l decoda (să spargi codul folosit). Chiar şi după 11 septembrie 2001, acest tip de „ascultare" s-a dovedit folositor în găsirea teroriştilor.

S-a dus vestea despre CARNIVORE, lucru de altfel de aşteptat (prea mulţi profesionişti în computere din afara FBI erau implicaţi în ţinerea lui sub secret) şi al-Qaeda a început să folosească mai multe mesaje de e-mail codate sau alte forme de comunicare. Cu toate acestea, veştile despre CARNIVORE au dus la un mare scandal în SUA când existenţa sa a devenit cunoscută în anul 2000. Deşi tehnica nu era nimic altceva decât o variantă modernă a dispozitivelor de ascultare, aplicată pe internet, foarte mulţi oameni au început să facă referiri la faptul ca Fratele cel Mare le citeşte e-mailurile. FBI a justificat existenţa programului CARNIVORE în faţa Congresului şi a publicului american prin următoarea declaraţie:

„Furnizorii de servicii online şi personalul lor sunt şi ei subiecţi ai legilor supravegherii electronice, însemnând ca supravegherea electronică neautorizată a clienţilor lor (sau a oricui altcineva) este interzisă, iar răspunderea penală şi civilă poate fi implicată de violarea drepturilor

cetăţeneşti. Nu numai că sunt interzise interceptările neautorizate, dar la fel este şi divulgarea conţinutului comunicaţiilor care au fost interceptate ilegal. Pentru acest motiv, printre altele, furnizorii de servicii online au foarte mare grijă să asigure asistenţă în îndeplinirea supravegherii electronice conform ordinului judecătoresc. În unele situaţii, furnizorii de servicii optează pentru oferirea de servicii «complete», în mod special ducerea la bun sfârşit a interceptării şi furnizarea rezultatului final al acesteia, dar, în multe cazuri, furnizorii sunt înclinaţi numai către oferirea nivelului de asistenţă necesar pentru a permite agenţiilor împuternicite de lege să efectueze interceptarea.

În ultimii ani, a devenit extrem de obişnuit ca FBI să ceară şi judecătorii să emită ordine pentru interceptări de Tipul III care sunt mai detaliate decât alte ordine ce vizează supravegherea serviciilor clasice de telefonie.

Pentru a fi implementate cu succes, acestea au nevoie de tehnici mai sofisticate pentru a ne asigura că numai acele mesaje pentru care există autorizaţie judecătorească sunt interceptate. Detaliile foarte multe din ordinele judecătoreşti se referă la două chestiuni.

Prima, complexitatea reţelelor de comunicaţii moderne precum internetul şi complexitatea comunicaţiilor utilizatorilor moderni cer o mai clară distincţie decât mai vechile comunicaţii analogice. De exemplu, utilizatorii de internet folosesc frecvent serviciile de mesagerie electronică precum e-mailul, pentru a comunica cu alte persoane într-o manieră care aminteşte de vechiul apel telefonic, folosind numai textul în locul vocii. Astfel de mesaje sunt de multe ori ţinta interceptărilor ordonate de justiţie. Utilizatorii folosesc şi servicii precum World Wide Web care arată mai mult ca o mass-media tipărită decât ca un apel telefonic. În mod similar, unele servicii de internet, ca de exemplu transmisiile video, au mai multe în comun cu televiziunea

decât cu un telefon. Aceste tipuri de comunicare devin într-o mai mică măsură ţintele unei interceptări.

În al doilea rând, pentru multe servicii de internet, utilizatorii împart aceleaşi canale de comunicaţie, adrese etc. Aceşti factori fac interceptarea mesajelor pentru care există autorizaţie judecătorească foarte dificilă. De aceea ordinele judecătoreşti conţin tot mai multe detalii pentru a elimina interceptarea comunicaţiilor care sunt în afara scopului ordinului.

Ca răspuns la o nevoie critică de instrumente pentru implementarea ordinelor judecătoreşti complexe, FBI a dezvoltat un număr de instrumente tehnice care sunt incluse în programul software numit «Carnivore». Acesta este un analizator de reţea specializat sau «adulmecător» care funcţionează ca o aplicaţie obişnuită pe un PC obişnuit ce foloseşte sistemul de operare Microsoft Windows. El «adulmecă» porţiunile potrivite de pachete din reţea, copiind şi înmagazinând numai acele pachete care se potrivesc unui filtru setat de program, în conformitate cu ordinul judecătoresc. Acest filtru poate fi extrem de complex, ceea ce conferă FBI-ului posibilitatea de a colecta transmisiunile care sunt în conformitate cu specificaţiile ordinelor judecătoreşti, de a urmări şi localiza suspecţi, de a face interceptări de Tipul III etc.

Este important să înţelegem ce am vrut să spun prin «adulmecare». Problema separării mesajelor utilizatorilor de pe internet este una complexă. Totuşi, asta este exact ce face Carnivore. Nu caută în conţinutul fiecărui mesaj, dar le colectează pe cele care conţin anumite cuvinte-cheie precum «bombă» sau «droguri». Selectează mesaje bazându-se pe criterii stabilite în ordinul judecătoresc, de exemplu, mesajele trimise sau primite de pe un anumit cont sau de la un anumit utilizator. Dacă programul este instalat la un anumit moment în reţea şi nu poate deosebi mesajele aşa cum este specificat în ordinul judecătoresc, pur şi simplu lasă toate mesajele să treacă neînregistrate.

Se pune întrebarea: «Ce sens are să mai folosim Carnivore atunci?» De multe ori, ISP-urile, mai ales cele mari, şi-au dezvoltat abilităţi care le permit să se conformeze parţial sau total ordinelor legale. De exemplu, multe ISP-uri pot «clona» sau intercepta, atunci când li se cere acest lucru în mod legal, e-mailurile de la sau către anumiţi utilizatori de conturi. În astfel de cazuri, aceste abilităţi sunt satisfăcătoare şi permit o aplicare totală a ordinului judecătoresc. Cu toate acestea, în cele mai multe cazuri, ISP-urile nu au astfel de abilităţi sau nu le pot pune în practică în condiţii de siguranţă. De asemenea, cele mai multe sisteme concepute de furnizorii de servicii online sau achiziţionate «de pe piaţa neagră» nu au capacitatea de a face diferenţa într-un mod corect între mesaje în conformitate cu ordinul judecătoresc. Mai mult, numeroase ordine judecătoreşti nu vizează doar e-mailul, specificând ca alte protocoale să fie interceptate, precum mesageria instant. În astfel de cazuri, o căsuţă poştală donată nu este suficientă pentru a fi în conformitate cu ordinul judecătoresc.

Acum, cred că este important să înţelegeţi cum este folosit Carnivore în practică. Mai întâi, există problema scării la care este utilizat. Acesta este un dispozitiv folosit la scară mică, numai atunci când este nevoie şi unde este nevoie. De fapt, fiecare dispozitiv Carnivore este depozitat în laboratorul FBI din Quantico până în momentul în care este nevoie de el. Este întrebuinţat pentru a satisface nevoia de informaţii a unui singur caz sau ordin judecătoresc şi ulterior, după expirarea ordinului, este scos din uz şi retrimis în Quantico.

Cea de-a doua problemă este legată de interferenţa reţelelor. Carnivore prezintă siguranţă atunci când este instalat pe reţele IP. Este conectat la un dispozitiv pasiv de colectare şi nu are nicio capacitate de a transmite ceva reţelei. De fapt, putem asigura faptul că sistemul nostru este izolat satisfăcător de reţeaua de care este ataşat. Mai

mult, Carnivore este ataşat la reţea numai după ce se solicită şi se obţine aprobarea personalului tehnic de la ISP.

De fapt, acest lucru ridică o a treia problemă – aceea a cooperării ISP-ului. Până acum, Carnivore nu a fost niciodată, din câte ştiu, instalat pe o reţea ISP fără asistenţă din partea personalului tehnic ISP. Internetul este un mediu extrem de complex şi eterogen pentru astfel de operaţiuni şi vă asigur că fără cunoştinţele tehnice ale personalului ISP ar fi foarte dificil, poate chiar imposibil, pentru agenţiile împuternicite de lege să implementeze cu succes şi să respecte cerinţele stricte ale unui ordin de interceptare. De asemenea, FBI depinde de personalul ISP pentru a înţelege protocoalele şi arhitectura reţelelor acestora.

Un alt motiv important pentru utilizarea sistemului Carnivore este integritatea datelor. Aşa cum ştiţi, Legea 901 din cadrul reglementărilor federale cere autentificarea dovezilor ca precondiţie pentru acuzare. Utilizarea sistemului Carnivore de către FBI pentru a intercepta şi înregistra comunicaţiile justifică o custodie neîntreruptă şi furnizarea unui martor ce poate depune mărturie pentru recuperarea dovezilor şi derularea procesului. Performanţa este un alt motiv esenţial pentru preferarea acestui sistem în locul «adulmecătorilor» de pe piaţă. Spre deosebire de software-ul acestora din urmă, Carnivore este creat pentru a intercepta şi înregistra comunicaţiile selectate în mod complet, fără «pachete omise».

În concluzie, aş vrea să menţionez că în ultimii cinci ani sau chiar mai mult, am fost martori la o creştere continuă a situaţiilor în care computerele au fost implicate în producerea infracţiunilor, incluzând aici infracţiunile tradiţionale şi activităţile teroriste care au fost plănuite şi duse la bun sfârşit folosind internetul. Capacitatea instituţiilor împuternicite de lege de a investiga eficient şi de a preveni aceste infracţiuni este, în parte, dependentă

de abilitatea noastră de a aduna dovezi ale acestor delicte, conform legii. Aşa cum internetul devine mai complex, la fel sunt şi provocările care ne revin de a menţine stabilitatea. Nu am putea face acest lucru fără cooperarea continuă a partenerilor noştri şi a inovaţiilor precum software-ul Carnivore. Aş vrea să pun accent pe faptul că FBI nu iniţiază interceptări, nu instalează şi nu activează programe de înregistrare şi nici nu foloseşte dispozitive de colectare şi înregistrare a datelor fără o autorizaţie legala din partea instanţei".

24 iulie 2000, declaraţie în faţa Congresului susţinută de Donald M. Kerr, director al Diviziei de Laboratoare, FBI

FBI merge deja mai departe decât în cazul Carnivore, cu un „adulmecător" de reţele pachet care poate accesa surse mai mari de date şi nu doar ISP-uri individuale. FBI crede că a susţinut o poziţie convingătoare în faţa judecătorilor privind legalitatea „adulmecării" ca fiind echivalentul unei interceptări telefonice pentru internet. De asemenea, FBI pune accent pe faptul că aproape două treimi dintre dispozitivele de interceptat sunt pentru aparatură wireless (în general telefoane, dar şi pagere şi altele asemănătoare) şi astfel îşi justifică cererea pentru un asemenea dispozitiv în cazul unei persoane (şi a tuturor căilor de comunicaţii pe care acea persoană le foloseşte).

FBI este ofensat de părerile pe care le primeşte de la grupurile de libertăţi civile în ceea ce priveşte dispozitivele de ascultare (care sunt puţine) şi lucruri precum CARNIVORE (care caută mesaje de la anumite persoane, nu e-mailurile tuturor). De asemenea, federalii ştiu că practic nu au resursele (oameni sau echipamente) necesare pentru a verifica prea multe e-mailuri. Şi din punct de vedere legal nu pot accesa decât mesajele oamenilor pe care curtea le permite să îi verifice. Mai mult, atunci când există cazuri în care se abuzează de

accesul FBI, de cele mai multe ori este vorba despre un funcţionar corupt care vinde informaţii infractorilor. Funcţionarul respectiv este de obicei condamnat şi trimis departe pentru o vreme. Între timp, fără lucruri precum CARNIVORE, au loc mai multe infracţiuni. Dar este de multă vreme la modă să vorbeşti cu emfază despre Fratele *cel* Mare şi acest lucru nu se va schimba prea curând.

CYBER-RĂZBOINICUL CEL MAI RAPID CÂŞTIGĂ

La fel ca şi armata, forţele aeriene americane implementează capacităţi de război informaţional de mare viteză. Pentru o lungă perioadă de timp, una dintre marile provocări ale forţelor aeriene a fost să detecteze, să focalizeze şi să atace apărarea inamicului cu rapiditate. Dacă forţele aeriene pot face asta mai repede decât îşi foloseşte inamicul armele, mai puţine avioane vor fi doborâte sau forţate să abandoneze atacul. Timp de decenii, avioanele speciale au fost folosite pentru detectarea şi atacarea radarelor din apărarea aeriană inamică. Asta înseamnă că un număr mare, de multe ori majoritatea avioanelor trimise să atace ţintele duşmane, erau acolo doar pentru a înfrunta apărarea aeriană a adversarului.

Dar tehnologia merge mai departe, iar acum forţele aeriene vor avea grijă ca fiecare avion de vânătoare sau bombardier din unitatea de atac să poată detecta radare şi asta cu o mai mare precizie. Acest lucru este făcut prin instalarea mai multor zeci de senzori în toate avioanele (inclusiv în avioanele-cisternă şi avioane de transport sau avioane de război electronic). Fiecare senzor detectează orice semnal radar care îl loveşte, la fel ca şi frecvenţa acestuia, direcţia şi ora exactă. Aceste informaţii împreună cu localizarea exactă a navei atunci când fiecare semnal a fost primit sunt transmise imediat (de multe ori printr-un satelit de comunicaţii) către un avion sau staţie de la sol

printr-un computer care preia informaţiile, calculează de unde a venit fiecare semnal (pană la 50 de picioare3) şi află ce fel de radar este. Apoi computerul poate ordona unui avion ce transportă proiectile sau bombe să lovească ţinta. Cum semnalele radar sunt de obicei preluate înainte ca avionul să intre în raza de acţiune a proiectilelor inamicului, computerul poate sfătui avionul dotat cu proiectile cu rază mare de acţiune să lanseze una asupra radarului. De asemenea armata are şi alte proiectile cu rază mare de acţiune (de la 160 până la 300 de kilometri) care pot face acest lucru. Chiar şi artileria poate fi folosită, dacă se află în zona de acţiune. Şi, în multe situaţii, artileria poate fi în apropiere (şi poate fi aceea care răspunde prima).

Mulţi inamici potenţiali au remarcat eficacitatea atacurilor americane asupra unităţilor antiaeriene inamice şi ştiu să îşi pornească radarele numai în ultimul minut. Această tehnică a fost folosită cu un oarecare succes de către sârbi în 1999 şi este bine cunoscută de către oricare alt posibil duşman. Astfel avioanele americane pot fi reperate şi poate fi trimis un proiectil asupra lor înainte ca apărarea americană să poată face ceva. Dar cu noul sistem, pe care nu îl vom vedea folosit încă vreo cinci sau mai mulţi ani, avioanele americane pot lovi orice radar înainte ca duşmanul să îşi stabilească ţinta. Acesta este un bun exemplu despre cum este aplicat războiul informaţional pentru folosirea armelor. Viteza ucide, mai ales într-un război informaţional.

CÂMPUL DE LUPTĂ AL INTERNETULUI

Atunci când a apărut World Wide Web la începutul anilor ’90, mulţi oameni au văzut utilizări inteligente ale acestei noi tehnologii. La fel şi armata americană, care a dezvoltat ideea unui câmp de luptă pe internet. Au numit-o „digitalizare” (a câmpului de luptă), un concept ce presupune instalarea unor monitoare în cele mai multe

vehicule de luptă şi comandă. Soldaţii individuali aveau să aibă „computere de corp” şi informaţiile aveau să fie afişate pe un dispozitiv asemănător unor ochelari. „Computerul de corp” este în lucru de câţiva ani, dar ecranul plat afişat în vehiculele blindate, avioanele şi sediile centrale este deja aici, la fel ca şi în dispozitivele cele mai bune de comunicare.

În luptă, informaţiile despre locul unde se află trupele inamice sau aliate, la fel ca şi poziţia câmpurilor minate sau a obstacolelor sunt probleme de viaţă şi de moarte. Noul echipament digitalizat permite trupelor să comunice mai uşor unele cu altele. Acum că ştii unde este toată lumea, nu mai auzi mesaje repetate la nesfârşit precum „unde eşti?” şi altele asemenea. Pentru că este vorba despre armată şi are loc o luptă, comunicaţiile sunt mai disciplinate decât cele obişnuite de pe chat. Chiar şi aşa, trupele au fost încântate de numărul tot mai mare de computere şi aparatură de comunicaţii. Spre sfârşitul anilor ’90, armata a experimentat instalarea echipamentelor computerizate în vehicule terestre şi avioane şi punerea în funcţiune a câmpului de lupta de pe internet.

În martie 2001, armata SUA a trimis 7.500 de trupe de la a patra divizie de infanterie la Centrul Naţional de Antrenament pentru a testa *cele* mai noi echipamente digitalizate. Trupele dispuneau acum de aparate de comunicare digitale care le permiteau să facă schimb urgent de date video, vocale sau scrise între vehiculele blindate, artilerie, avioane, infanterie şi sedii centrale. Ideea era de a avea o forţă de luptă care poate reacţiona mai rapid decât inamicul. Prin atacarea ţintelor mai repede, duşmanul cade într-un mare dezavantaj. Dintotdeauna, transmiterea informaţiilor despre inamic către comandant a fost o problemă pentru soldaţi. Forţa digitalizată rezolvă asta. Comandantul ştie mereu unde sunt propriile trupe şi obţine informaţii mai bune despre

adversar într-un timp mai scurt. Impactul va fi similar cu ceea ce s-a întâmplat când maşinile de poliţie au primit radiouri acum vreo 50 de ani. Dintr-odată, o infracţiune precum jaful unei bănci a devenit mult mai periculoasă. Odată ce era raportată o infracţiune, poliţia putea folosi rapid radioul pentru a chema întăriri şi putea primi informaţii de la martori sau, să zicem, poliţişti pedeştri care îi văzuseră pe jefuitori în flagrant delict. Radioul singur nu a revoluţionat războiul la fel de mult pentru că bătăliile sunt un proces mult mai complex şi mai haotic

Digitalizarea şi folosirea computerelor plus soldaţii care au ani de experienţă pe internet vor face o mare diferenţă. Dar un alt motiv pentru care armata a fost nerăbdătoare să testeze unităţile digitalizate în condiţii de luptă a fost ca să descopere acele lucruri pe care nu le luaseră încă la cunoştinţă. Noi forme de război tind să creeze oportunităţi şi capcane pe care nimeni nu le-a prevăzut. Aşa cum multe armate s-au împiedicat de războiul „fulger” de la sfârşitul anilor ’30 şi începutul anilor ’40 cu rezultate inegale, acelaşi lucru se aşteaptă să se întâmple cu digitalizarea, atunci când această tehnologie va intra pe câmpul de luptă.

Armata pune accent pe nerepetarea aceloraşi greşeli întâlnite în trecut, când au fost introduse tehnologii complet noi. Ideea de a le oferi trupelor un internet pe care să îl poată folosi chiar pe câmpul de luptă poate fi o mare realizare sau un dezastru major. La Centrul Naţional de Antrenament, unde au loc exerciţii de luptă foarte realiste, trupele au avut tendinţa să creadă că ştiu unde se află totul şi s-au concentrat pe a-l lua prin surprindere pe inamic. Teoretic, este un lucru bun. Digitalizarea îi conferă utilizatorului un avantaj informaţional. În vreme ce inamicul încă mai încearcă să îşi dea seama cine pe unde se află, forţa digitală ştie unde este toată lumea şi execută un atac zdrobitor. În realitate nu toate informaţiile de pe ecran erau corecte şi actualizate, iar acest lucru a dus la

unele explozii minore, dar jenante, la Centrul Naţional de Antrenament. Acest lucru s-a întâmplat când ecranul computerului spunea că se află un tanc inamic acolo, dar de fapt era un vehicul aliat. Trupele au avut probleme şi cu pătrunderea în câmpuri minate sau drumuri blocate pe care nimeni nu le-a găsit în baza de date. Aceste situaţii pot fi caracterizate ca fiind bătăi de cap date de noua tehnologie. Dar de asemenea arată că tehnologia digitalizată funcţionează cel mai bine, asta dacă funcţionează, numai cu trupe instruite şi disciplinate. Aşa cum experienţa pe internet îţi permite să faci lucrurile mai repede (ca utilizarea unui motor de căutare sau setarea unui chat room), şi trupele vor petrece mult timp folosindu-şi tehnologia pe câmpul de luptă al internetului astfel încât să o poată exploata eficient. Cei mai mulţi membri ai trupelor de azi au crescut cu videoclipuri şi jocuri pe calculator. Şi asta i-a învăţat o lecţie periculoasă. Jocurile pe computer arată aproape întotdeauna informaţii clare. Ceea ce vezi este ceea ce trebuie să înfrunţi. Pe câmpul de luptă, lucrurile nu sunt la fel de bine stabilite. De fapt, să ştii să evaluezi informaţii ambigue (ceea ce vezi pe ecranul computerului nu este neapărat realitatea) este una dintre acele abilităţi necesare supravieţuirii în luptă. Aşa că generaţia Nintendo trebuie să scape de unele obiceiuri proaste înainte de a putea face faţa câmpului de luptă digitalizat.

Războiul din Afganistan a fost un test parţial pentru digitalizare, în primul rând pentru că nu toate echipamentele digitale existau şi atunci. Dar o mare parte dintre ele erau, iar rezultatele au fost destul de spectaculoase. De asemenea, forţele aeriene au lucrat, pe parcursul anilor ’90, la propria versiune de digitalizare {care deja se potriveşte cu o parte din digitalizarea armatei). Obiectivul forţelor aeriene era să poată lovi ţintele la mai puţin de zece minute după ce le vedeau. De ce zece minute? Pentru că în timpul Războiului din Golf din

1991, în încercarea fără succes de a găsi şi iovi lansatoarele de proiectile irakiene aveau nevoie, se pare, de un timp de reacţie de zece minute (între stabilirea ţintei lansatorului şi ajungerea bombei la aceasta). Irakienii aveau nevoie de cel puţin zece minute pentru a pleca de acolo, aşa că dacă i-ar fi lovit într-un timp mai scurt de atât, i-ar fi putut distruge. Aşadar nu este nimic magic la cele zece minute, este doar un număr bazat pe ceea ce îţi trebuie pentru a lovi un anumit tip de ţintă. Grupurile mici de tancuri sau camioane pot elibera o zonă în câteva minute, dacă ştiu că au fost localizate. Dar acest context le-a oferit forţelor americane un scop.

În Afganistan, digitalizarea forţelor aeriene a însemnat sisteme de recunoaştere (sateliţi, avioane, JSTARS, avioane teleghidate) pentru a găsi ţinte, un avion de comanda (unde se afla un tip care putea autoriza atacurile, renunţând la avocaţii şi politicienii care au încetinit lucrurile în Kosovo şi în Războiul din Golf) şi bombardiere în apropiere pregătite să lanseze o bombă inteligentă care să poată lovi ţinta. Mai întâi această abordare a fost folosită în Afganistan pentru a distruge vehiculele militare aflate în mişcare. A funcţionat destul de bine şi în destul de scurt timp talibanii stăteau în afara drumurilor atunci când credeau că sunt bombardiere americane prin apropiere. Apoi a venit impulsul din partea războiului terestru. Acesta a folosit trupele speciale americane şi controlorii de la sol ai forţelor aeriene pentru a comunica direct cu bombardierele de deasupra. Tipii de la sol foloseau un laser pentru a „lumina” ţinta pentru bombă sau navigaţia GPS prin satelit pentru a localiza ţinta şi a trimite acele coordonate bombardierului, moment în care coordonatele intrau într-un sistem de navigaţie prin GPS şi bomba era lansată. La început, forţele aeriene au crezut că pot trimite bombele spre ţinte în 11 minute. La sfârşitul anului 2001, făceau acest lucru în mai puţin de 10 minute.

Unele dintre sistemele de detecţie şi de comunicaţie folosite în Afganistan erau improvizate. Se construiau dispozitive mai uşor de folosit, cumpărate sau puse în mâinile trupelor în anul 2002. Aceste dispozitive erau o combinaţie între binoclu şi un detector laser care capta locaţia exactă a ţintei şi o transmitea direct către bombardierul de deasupra, unde coordonatele erau introduse într-o bombă ghidată prin GPS. Echipajul bombardierelor dispune de ecrane de computer care pot arăta locaţia detectoarelor de ţinte de la sol şi locul unde va fi trimisă bomba, deşi computerul avionului poate de asemenea să calculeze rapid dacă bomba este prea aproape de trupele aliate. Uneori nu se poate face nimic şi cei de la sol trebuie să anunţe echipajul bombardierului că va fi o lovitură la mică distanţă de ei.

Experienţa din Afganistan a demonstrat un alt aspect al modului în care armata foloseşte tehnologia. Pe câmpul de luptă, trupele pot improviza. Ei numesc asta „eficacitate pe câmpul de luptă”, pentru că, atunci când îţi este pusă viaţa în pericol, tinzi să fii foarte creativ cu ceea ce ai. În ultimele două decenii, tot mai multe trupe şi-au luat computerele personale şi alte aparaturi în luptă sau operaţiuni de instruire. Departamentul Apărării depinde de faptul că trupele vor improviza atunci când va începe focul şi vor inova pe câmpul de luptă al internetului. Bazându-ne pe experienţele trecute, probabil acesta este modul în care se vor desfăşura lucrurile.

Tehnologia câmpului de lupta al internetului nu este numai pentru trupele de război. Aceeaşi tehnologie este introdusă peste tot în armată, la fel cum a fost răspândită în toate organizaţiile, de la angajaţii fabricilor la avionul cu reacţie al unui CEO. La sfârşitul anului 2000, armata americană a pus poliţia militară să testeze un nou sistem „MP digital”. Acesta este format dintr-un computer portabil şi o pereche de ochelari speciali care conţin o cameră video ce trimite un flux constant de imagini cu

ceea ce MP (poliţia militară) priveşte. În interiorul uneia dintre lentile este un monitor (la fel ca cele disponibile pentru jocuri). Acest ecran poate afişa date sau imagini, practic orice ai vrea să vezi pe un ecran obişnuit de calculator (deşi rezoluţia nu este la fel de bună, ci doar 480 până la 640). De exemplu, un MP poate căuta, folosind comenzi vocale sau un ID introdus pe o tastatură portabilă (purtată pe braţ aşa cum există în prezent pentru costume spaţiale), fotografii cu oameni urmăriţi sau fotografia din dosar atunci când suspectezi că cineva din sistem încearcă să intre cu un ID fals. Sistemul MP digital este creat pentru a oferi poliţiei militare acces la mai multe informaţii, ceea ce în ultimul secol s-a dovedit a fi cea mai mare achiziţie din arsenalul unui poliţist. Acest lucru este adevărat în mod specia] pentru operaţiunile antiterorism unde sunt folosite foarte multe ID-uri false pentru a-i duce pe băieţii răi în locuri unde nu ar trebui să se afle. Ansamblul digital MP include şi o „carte digitală” de mărimea unui PDA care conţine documente suplimentare de care MP s-ar putea să aibă nevoie. Acest dispozitiv a fost creat şi pentru soldaţii din infanterie, dar problemele legate de rezistenţa şi durata bateriilor au făcut ca dispozitivul să nu fie practic pentru acest tip de muncă. Dar pentru un MP care nu se mişcă la fel de mult ca un infanterist şi tinde să fie mai aproape o rezervă proaspătă de baterii, sistemul funcţionează, iar în viitor va fi creat un sistem mai de încredere pentru a fi folosit de infanterie.

Dar aceste dispozitive wireless pentru câmpul de luptă al internetului au toate o mare vulnerabilitate: posibilitatea de a fi sparte. Din nefericire, este nevoie şi de securitate pe internet, odată cu numărul tot mai mare de aparate wireless pe care le folosesc oamenii. Aici sunt incluse telefoanele mobile, PDA-urile şi dispozitivele de e-mail (precum Blackberry). Desigur, atunci când acestea au fost vândute pentru prima dată, producătorii au spus că vor rezista în faţa hackerilor. S-au înşelat şi acum

securitatea internetului wireless este o mare afacere. Armata va cumpăra o versiune a celei mai robuste securităţi wireless disponibile (care foloseşte o formă de coduri). Dar militarii tot vor fi vulnerabili, deşi inamicul va fi nevoit să muncească mai mult pentru a sparge aceste sisteme. Cea mai mare problemă în privinţa căreia ar trebui să fie îngrijorate trupele este bruierea (o versiune wireless a atacului DDOS) care va acoperi mesajele wireless cu zgomot electronic.

În timp ce SUA deţin supremaţia cu tehnologia digitalizată, alte naţiuni o adoptă şi ele. În anul 2000, armata franceză a adoptat un sistem de informaţii digital pentru recunoaşterea vehiculelor, tancurilor şi vehiculelor antitanc. Suedia a demonstrat un alt aspect al digitalizării. A început să dezvolte o astfel de tehnologie în anii ’70 pentru forţele aeriene, dar a ţinut secret acest lucru. Suedezii şi-au dat seama că nimeni altcineva nu mai lucrează la aşa ceva şi au realizat că, dacă sunt singurii care o au, vor avea o forţă aeriană mult mai eficientă decât inamicul lor probabil, Rusia. Acest lucru scoate în evidenţă un alt aspect al noii tehnologii militare. Dacă ai ceva nou şi duşmanul ştie despre asta, pot fi dezvoltate contramăsuri. Sau în cazul digitalizării luptei aeriene, pot construi acelaşi sistem pentru propriile avioane şi îţi vor anula avantajul. Aşa că, dacă poţi, ţine secrete lucrurile noi. Ruşii au folosit cu succes această abordare înainte de cel de-al Doilea Război Mondial lansând noi arme despre care germanii nu ştiau nimic şi înregistrând o mare reuşită. SUA au făcut acelaşi lucru cu avioanele invizibile (nedetectabile prin radar) pe care le-au ţinut ascunse până au fost puse în funcţiune. La sfârşitul Războiului Rece a fost dezvăluit faptul ca ruşii au dezvoltate mai multe arme (torpile de mare viteză, proiectile şi altele similare) despre care nimeni din Occident nu ştia nimic.

Chiar şi canadienii, care multă vreme au fost zgârciţi cu cheltuielile militare, au comandat un nou sistem de

mesagerie militară pentru 26 de milioane de dolari şi au adoptat cu entuziasm tehnologia internetului pentru uz militar. Ţări precum Canada şi China, cărora nu le place (sau nu îşi pot permite) sa cheltuiască bani pentru tehnologie militară, au descoperit că este mult mai ieftin şi mai eficient să adaptezi tehnologia nouă a internetului pentru utilizare militară. Computerele personale şi internetul se dovedesc a fi, pentru armată, cea mai puternică tehnologie pe care au întâlnit-o vreodată.

Pentru majoritatea naţiunilor, digitalizarea aparatelor costă mai mult decât vor să cheltuiască pentru forţe pe timp de pace. Dar acest lucru se schimbă pe măsură ce văd forţele americane operând mult mai eficient cu aparatura digitala. În timpul Războiului din Kosovo din 1999, a existat o diferenţă clară de eficacitate între forţele aeriene americane şi cele europene. Bombele inteligente americane şi aparatura electronică superioară erau mult mai puternice decât cele pe care le aveau europenii. Nu era un secret că europenii nu aveau aceleaşi arme inteligente şi aparatură de înaltă performanţă pe care o foloseau avioanele de război din SUA, dar pentru mai bine de un deceniu, europenii încercaseră să se convingă singuri că toate acele aparate ale yankeilor sunt supraestimate şi nu merită cheltuiala. Ups!

Este adevărat că vei plăti mai mult şi vei avea mai multe dificultăţi de înfruntat dacă vrei să fii primul care are cele mai noi tehnologii şi echipamente. Oricine s-a grăbit să cumpere cel mai nou tip de aparat electronic cunoaşte sentimentul. Un nou tip de computer, camera video sau reţea wireless, toate vor costa mai mult şi vor prezenta mai puţină siguranţă decât dacă aştepţi un an sau doi. Dar aşteptarea poate fi fatala când vine vorba de echipament militar. Aliaţii noştri europeni au aflat acest lucru în timpul campaniei de bombardamente din Kosovo, în 1999. Noi eram acolo pentru a deturna ţintele, deoarece tehnologia europeană mai puţin performantă a avioanelor

ar fi periclitat succesul operaţiunilor. Europenilor nu le place să spună cu voce tare că tehnologia militară americană a salvat viaţa multor piloţi de-ai lor, dar aşa s-a întâmplat. Şi s-a întâmplat din nou în Afganistan. Veteranii ruşi ai războiului lor din anii ’80 au spus iniţial că afganii vor înfrânge trupele americane şi se vor dovedi nişte adversari formidabili. După ce au văzut cum funcţionează noua digitalizare, cu trupele speciale terestre folosind radiouri speciale, detectoare cu laser şi aparatură GPS şi cu forţele aeriene cu bombe GPS, veteranii ruşi tindeau să remarce înţelept: „Dacă am fi avut şi noi aşa ceva…”

COLOR ŞI GHIDAT PRIN SATELIT

Unul dintre mulţii paşi înainte pe care războiul informaţional i-a adus este abilitatea de a oferi trupelor tehnologie care este mai ieftină şi mai puternică datorită numărului mare de civili care folosesc acelaşi echipament. În acest caz, ecranele computerelor. În ultimii ani, utilizatorii de PC au remarcat, cu oarecare plăcere, că ecranele computerelor devin mai mari, mai uşoare şi mai ieftine. Ei bine, varianta mai uşoară (ecranul plat) te va costa în plus. Dar chiar şi acesta devine mai ieftin.

Trupele au nevoie de astfel de lucruri. Gândeşte-te la asta: sunt mai multe trupe se luptă uitându-se la un ecran decât numărul infanteriştilor, Bine ai veni în secolul XXI.

Nimeni de la Departamentul Apărării nu va spune dacă reclamaţiile trupelor cu privire la multele lucruri nesemnificative (ecranele monocrome încă instalate în tancuri, avioane, nave şi posturi de comandă) au ceva de-a face cu toate astea. Dar sunt numeroase acele actualizări ale echipamentelor care implică instalarea ecranelor color, de multe ori mai mari, în echipamentele militare. Adevăratul motiv este că de-a lungul anilor armata a făcute cercetări intense despre „ingineria umană” şi a descoperit că generaţia de trupe crescută cu PC-uri şi jocuri video este mult mai eficientă dacă are la dispoziţie un ecran mai

mare şi mai colorat. Cu cantitatea mai mare de informaţii generată de sateliţi, avioane cu pilot automat, camere video şi mulţi alţi senzori, este uşor să ratezi ceva când toate invadează ecranul. De multe ori, prea multă informaţie creează confuzie şi devine contraproductivă. Dar aşa cum a aflat Wall Street în anii ’80, dacă ai grijă când proiectezi modul în care sunt distribuite lucrurile pe ecran, devii mult mai eficient.

Cu toate acestea, există un element critic în legătură cu care trupele trebuie să îşi facă griji şi cei de pe Wall Street nu: unde se află? Sistemul de navigaţie bazat pe sateliţi GPS tocmai îşi făcea apariţia online când a izbucnit Războiul din Golf din 1991. Dispozitivele erau relativ scumpe. În ciuda preţului ridicat şi a performanţei mai puţin importante, GPS-ul a avut un mare succes în rândul trupelor. Această poveste de dragoste a continuat. Unităţile sunt atât de ieftine acum (unele noi coboară şi sub 100 $) încât de multe ori trupele cumpără unul în plus în caz că cel asigurat de guvern se strică. De asemenea, a fost observat faptul ca de multe ori trupele merg la exerciţiile de antrenament cu un laptop echipat cu GPS şi un sistem de hărţi ce foloseşte CD-ROM-uri. Acest lucru a atras atenţia oficialităţilor. Evident, trupele de rang inferior au fost primele care au avut ideea acestei metode de navigare neoficiale. Desigur, combinaţia laptop/GPS este o inovaţie comercială de la mijlocul anilor ’90. Dar a ajuns atât de ieftină încât majoritatea maşinilor noi o vor avea în următorii ani (acum este echipament opţional). Sistemul este foarte comun pentru automobilele japoneze (în Japonia, unde numerele clădirilor sunt alocate în general în funcţie de cel care construieşte primul pe o stradă, şi nu mergând dintr-un capăt al străzii către celălalt).

Sistemele de cartografiere militară sunt un pic diferite, întrucât arată şi locaţia vehiculelor aliate. Acest lucru se poate realiza pentru că fiecare vehicul transmite

în permanenţă locul în care se află (conform GPS-ului) faţă de vehiculele din apropiere. Mai există o versiune în lucru care va arăta şi ultima poziţie raportată a vehiculului inamic. Au existat teste ale sistemelor care permit ca aceasta informaţie să fie trimisă la sediile centrale şi la avioanele de deasupra. Acest lucru face ca tancurile şi avioanele să fie mult mai eficiente şi reduce risipirea muniţiei aliaţilor.

Marina americană a adoptat ecranul color ca instrument al războiului informaţional datorită numărului mare de fani Star Trek care au devenit amirali în cele din urmă. Acestor amirali nu le place întotdeauna să vorbească despre acest aspect, deşi au mai scăpat informaţii din când în când. Dar văzând cât de uşor era comandată o navă ficţională dintr-o cameră plină de ecrane, au fost create diferite modele în ultimele două decenii. Cel mai recent efort este o navă de comandă echipată cu un „zid al cunoaşterii”. Acesta constă într-o serie de monitoare care arată situaţia navelor, avioanelor şi vehiculelor amfibie. Pe lângă hărţi şi date, sistemul poate încorpora şi teleconferinţa. Cum preţurile scad pentru ecranele mai mari, acestea sunt cele instalate. Folosirea ecranelor plate, chiar dacă sunt mai scumpe, de fapte duce 3 a economisire. Utilizarea unui număr mare de tuburi catodice generează prea multă căldură pentru aerul condiţionat de pe nave. Înnoirea aparatelor de aer condiţionat costă prea mult, aşa că ecranele plate, care emană mai puţină căldură şi consumă mai puţină energie, permit achiziţionarea unui număr mai mare de monitoare fără a fi nevoie de schimbarea aparatelor de aer condiţionat.

Mai multe ecrane mari sunt esenţiale din cauza cantităţii mari de informaţii care intră în sistem. Sateliţii, UAV-urile şi avioanele de recunoaştere pot trimite acum imagini video în timp real şi alte informaţii electronice. E-mailurile primite de la nave şi submarine au devenit ceva

standard, având în vedere toţi marinarii cărora le este dată o adresă de e-mail atunci când se înrolează. Marina foloseşte de asemenea şi telefoane mobile şi PDA-uri wireless la bord. Toate aceste aparate pot trimite informaţii către centrul de comandă şi către zidul cunoaşterii. Aici ai parte de un război informaţional ca exerciţiu de grup. În faţa zidului cunoaşterii lucrează peste o duzină de ofiţeri şi experţi tehnici. Pe măsură ce apar informaţiile, apar şi oportunităţi, probleme şi potenţiale soluţii. Grupul acţionează împreună, făcând schimb de idei, rezolvând rapid problemele şi profitând de oportunităţi. Aceste sisteme de informaţii sunt considerate acum atât de vitale încât exerciţiile şi testele de azi includ situaţii în care trebuie să faci faţă atacurilor asupra sistemelor de informaţii ale navei. Da, chiar şi în mijlocul oceanului, flota este îngrijorată cu privire la hackerii răi care ar putea provoca pagube. Dar cel mai important este să exersezi cum să funcţionezi după ce nava este lovită de un proiectil şi o parte din sistemele războiului informaţional intră în avarie.

De fapt, flota a fost prima care a dezvoltat conceptul de „structură multimedia” a sediilor centrale. În timpul celui de-al Doilea Război Mondial, a fost creat Centrul de Informaţii de Luptă. Nu existau ecrane de tip televizor, televiziunea era de-abia la început pe atunci. Dar nişte panouri mari (cu poziţia avioanelor şi navelor) erau pe atunci actualizate manual pe baza transmisiilor audio; ulterior au fost introduse şi alte dispozitive. Englezii au folosit un sistem similar pentru a purta Bătălia Angliei din 1940. Aceasta campanie a implicat de multe ori peste o mie de avioane în acţiune în acelaşi timp. Fiecare sediu central de azi are computere şi cele mai multe dintre ele au un program de grafică ce arată ce se petrece pe câmpul de luptă. În timpul Războiului din Golf, un anumit joc de război al Departamentului Apărării a fost folosit doar pentru abilitatea lui de a afişa situaţia tactică (exista o mai

puţină încredere în capacitatea de predicţie a jocului în sine).

Nu numai că ajunge mai multă informaţie la comandanţi, dar numărul detaliilor creşte (calitatea este adăugată la cantitate). Unul dintre mani fani ai HDTV (High Definition TV, care în curând va fi un standard naţional) este armata. HDTV, spre deosebire de camerele de televiziune folosite în prezent pentru recunoaşterea avioanelor, UAV-urilor şi chiar şi a trupelor terestre, este o tehnologie oarecum confuză. HDTV aduce mai multe detalii şi claritate. Acest lucru permite computerelor să deceleze elementele de înşelătorie şi să calculeze lucruri precum viteza vehiculelor sau a avioanelor care apar în imagine.

La sfârşitul anului 2000, flota americană a început să modifice USS Coronado, nava-comandant a celei de-a Treia Flote, pentru a o echipa cu o mare parte dintre jucăriile noi ale războiului informaţional. Această navă a slujit ca „laborator” pentru testarea acestor lucruri noi de management al informaţiei în luptă, înainte ca ele să fie instalate şi pe restul navelor.

Totul se învârteşte în jurul informaţiei, nu doar la a o avea, ci şi la a o expune clar, pentru ca trupele să poată vedea ce se întâmplă atunci când sunt în situaţii dificile. Este ca un joc pe calculator. Dar dacă pierzi, mori cu adevărat. De aceea, unul din considerentele de proiectare ale acestor sisteme este să fie rezistente în faţă hackerilor. Aşa cum a fost descoperit în cazul internetului, spargeri posibile (discutate în perioada de început a internetului), au deveni în cele din urmă reale. Pe câmpul de luptă, o spargere a reţelei de informaţii militare poate face rapid ca situaţia să devină fatală.

AIRNET ŞI INFORMAŢIA VENITĂ DE SUS

Armata SUA a îmbrăţişat războiul informaţional pe câmpul de luptă, dar are probleme cu obţinerea întregului

echipament de care are nevoie (sau, după cum se pare uneori, nu are nevoie). La sfârşitul anului 2000, au scăzut la jumătate cheltuielile de achiziţie a elicopterelor A2C2S (Army Airborne Command and Control System). De asemenea, a amânat introducerea unor mitraliere modernizate UH-60 din 2000 până în 2004.

Aceste elicoptere trebuie folosite ca posturi aeriene de comandă pentru comandanţii de brigadă şi de divizie. Începând cu Vietnam, trupele au urât imaginea unui comandant zburând pe deasupra într-un elicopter, pentru că de obicei însemna că bătrânul vedea probabil câmpul de luptă cu binoclul şi critica subofiţerii şi ofiţerii de la sol. Fără să ştii, te trezeşti că ai un general la radio care îţi spune să te deplasezi un pic spre nord şi să alergi prin pădure. Generalul nu ştie, desigur, că în pădure este o mică mlaştină şi nicio cărare. Dar, hei, arată atât de liber şi simplu de acolo de sus… Aceasta este partea rea în a avea prea multe informaţii greşite. Chiar şi generaţia de ofiţeri care abia fusese promovată în timpul Războiului din Vietnam pare să uite că, de îndată ce au devenit generali, toţi au obţinut un elicopter şi au început să îşi trateze trupele ca pe nişte soldaţi de jucărie într-o cutie de nisip. Aşa arată partea întunecată a războiului informaţional. Recunoscând problema şi realizând că toţi generalii au crescut cu reluări ale serialului *Star Trek,* armata a decis să profite de noile bunătăţi electronice şi a încercat să le îndese pe toate într-un elicopter Black Hawk (UH-60). Acest lucru i-ar permite comandantului să adune informaţii dintr-un număr mai mare de surse (sateliţi, avioane de recunoaştere, trupe terestre) dar şi să ştie unde se află trupele lui în fiecare moment. Instalarea aparaturii pe un UH-60 alături de echipajul cu mitraliere şi alte câteva persoane subordonate i-a permis comandantului să fie mai mobil şi mai puţin în pericol de a fi ucis. Cartierele generale au fost în mod deosebit vulnerabile în faţa proiectilelor şi atacurilor aeriene, din cauza volumului

mare de mesaje electronice care erau trimise. Toate acele transmisii au făcut ca, în jargon, cartierele generale să fie numite

„Magneţi de proiectile”. Având aproximativ o jumătate de duzină de elicoptere A2C2S pentru fiecare divizie, acestea au devenit o ţintă mai dificilă. Această abordare a permis de asemenea comandantului să îşi viziteze personal unităţile subordonate, ceea ce este întotdeauna un lucru bun, de care este şi mai mare nevoie din cauza dependenţei tot mai mari a subordonaţilor faţă de informaţiile electronice.

Dar războiul nu este un joc video, iar elementului uman trebuie să i se acorde atenţie şi acest lucru se face cel mai bine personal. Îndeplinirea acestui program ambiţios depindea de nişte contractori care trebuiau să aibă noul echipament gata la timp sau disponibil în variante mai simple.

Dând probabil vina pe Y2K, contractorii au ratat termenele-limită. Atunci când va fi dat în cele din urmă în funcţiune, A2C2S va fi dotat cu cinci staţii de lucru computerizate. Ecranele plate şi microprocesoarele mai puternice fac posibil acest lucru. A2C2S este o altă componentă din programul de digitalizare al armatei, care va permite vehiculelor de luptă şi comandanţilor să aibă un schimb de informaţii instant despre locul în care se află şi datele pe care le cunosc despre inamic. Acest lucru măreşte abilitatea trupelor americane de a găsi şi lupta cu inamicul. A fost dintotdeauna un mare avantaj să ai o forţă mai rapidă, exceptând elementul negativ al micromanagementului. Nimeni nu ştie sigur cum se vor rezolva toate acestea în luptă, dar puţini generali de pe planetă vor să fie ultimii care să aibă acces la câmpul de luptă al inter netului.

ŞUETĂ MILITARĂ

La sfârşitul anului 2001, Marina Regală Britanică a

reunit pentru exerciţii în Golful Persic cea mai mare forţă de nave de război de la Războiul din Insulele Falklands din 1982. Forţele includeau o bază a aviaţiei, 2 distrugătoare, 4 fregate, 2 submarine nucleare, 2 nave amfibie, 5 dragoare şi 11 nave de rezervă. Aviaţia mobilizată includea 15 aeronave Harrier şi 25 de elicoptere. Aproximativ 8.500 de marinari erau implicaţi. Ceea ce a făcut acest exerciţiu cu adevărat diferit a fost utilizarea intensă a internetului. Fiecare navă avea propriul intranet (o structură de reţea ce poate opera fără acces la nimic din afara navei), dar şi conexiuni criptate la internet între nave. În loc să folosească radioul pentru comunicare, s-a folosit foarte mult chatul. Dar spre deosebire de un chat room public, Marina a folosit obişnuita „disciplină a netului" (care precede internetul de mai bine de jumătate de secol), astfel încât mesajele importante să nu fie pierdute în discuţii. O unitate de comando a navelor are nevoie de foarte multă comunicare între nave pentru a ţine operaţiunea în desfăşurare. Marea parte a acestor lucruri nu apare în filmele despre operaţiuni navale, pentru că ele nu înseamnă de fapt nimic pentru public. Este vorba despre multe materiale tehnice, dintre care cea mai mare parte este formulată în jargon. Cele mai multe nu trebuie trimise în mare grabă, aşa că marinarii din fiecare navă au destul timp la dispoziţie pentru a tasta mesajele pe chat. Acest lucru oferă avantajul înregistrării detaliilor: cine ce a zis şi când (aceste spaţii secretizate de chat salvează toate convorbirile într-un fişier şi pentru fiecare mesaj al fiecărei persoane este afişată ora la care a fost trimis). Radioul este încă disponibil pentru mesajele urgente. De fapt, radioul este chiar mai liber pentru mesajele urgente întrucât majoritatea acestor mesaje sunt acum tastate. Dacă un marinar aude că soseşte un mesaj prin radio, ştie că este foarte important şi nu doar ceva administrativ de genul „apropie-te cu 3 kilometri şi redu viteza la 15 noduri". Mai mult, odată ce sunt rezolvate toate

problemele, poţi folosi cu uşurinţa transmisia de alte date digitale, precum hărţi şi informaţii despre forţele inamice.

În plus, internetul este o tehnologie de comunicaţii valoroasă pentru că aproape fiecărui recrut îi este deja familiar. Este ieftin, securitatea este destul de bună (deşi majoritatea utilizatorilor civili nu îşi fac probleme în acest sens) şi este foarte flexibil. De obicei, navele sunt la destul de mare distanţă de inamic pentru a face dificilă bruierea sau spargerea traficului pe internet de la o navă la alta.

EXPERŢII ÎN PROIECTILE PE CÂMPUL DE LUPTĂ AL INTERNETULUI

Ideea de a folosi internetul pe câmpul de luptă a prins contur chiar înainte de existenţa internetului. Când au fost date în folosinţă telefoanele şi radioul în timpul Primului Război Mondial (1914 – 1918), militarii mai grijulii au observat cum aceste noi aparaturi electronice permit informaţiei să traverseze mult mai repede haosul de pe câmpul de luptă modern. Dar toate astea erau în stadiul de teorie, pentru că liniile telefonice erau deseori întrerupte pe câmpurile de luptă din Primul Război Mondial, iar radiourile de atunci nu erau foarte portabile. Dar până la începerea celui de-ai Doilea Război Mondial (1939 – 1945), apăruseră destul de multe radiouri portabile. Chiar şi înainte, în anii ’30, ofiţerii artileriei americane au găsit o modalitate de a obţine printr-un radio sau telefon mesaje de oriunde, pe o distanţă de mai multe mile de-a lungul liniei de front, de la cineva care dorea deschiderea focului asupra unei ţinte aşa încât, în mai puţin de o oră, sute de arme de artilerie să lovească acea ţintă. Această minune a anilor ’40 a băgat spaima în germani, dar era nevoie de multă muncă. Nu existau computere care să facă toate calculele necesare, iar persoana din faţă putea face o greşeală fatală atunci când raporta poziţia ţintei

Mergem cu paşi repezi spre 2001 şi dealurile aride

din nordul Afganistanului. Trupele au radiouri mai bune şi alte dispozitive electronice pentru evidenţierea locaţiei ţintelor. Aliaţii noştri afgani sunt amuţiţi de modul în care americanii pot vorbi la un radio, apasă câteva butoane şi apoi, în numai câteva minute, culmea de la aproape o milă depărtare dispare cu un vuiet şi un nor de praf. Inamicul a fost acolo, dar nu mai este. Numai dacă nu iei în calcul părţile corpului uman împrăştiate într-un crater larg.

Şi asta nici măcar nu era lucrul la care se gândeau tipii inteligenţi în timpul anilor ’90. Ideea lor, numită NetFires, este încă în lucru. Acest sistem a fost creat de către armată şi nu depinde de forţele aeriene. Dar depinde de un câmp de luptă pe internet care va face ca toţi băieţii buni să ştie unde se află cei răi. Pare uşor, pentru că tehnologia internetului se îmbunătăţeşte în permanenţă şi lucrurile sunt repede dezvoltate de milioane de utilizatori pasionaţi. Armele care ar profita de pe urma tuturor acestor informaţii sunt o altă problemă. Chiar şi cu viteza internetului, ţintele importante, precum tancurile, se pot mişca în continuare. De aceea, pentru ca acest câmp de luptă al internetului să funcţioneze, trebuie să poţi lovi ţintele aproape imediat ce le vezi.

Pentru a ucide, au fost create două noi proiectile. Principalul este PAM (Precision Attack Missile). PAM este un proiectil cu un diametru de 178 de milimetri care cântăreşte 45 de kilograme şi are o rază de acţiune de 50 de kilometri. PAM atacă de sus cu un focos de 12 kilograme. Astfel poate nimici orice tanc, lovind partea mai subţire a blindajului. PAM-urile sunt lansate pe verticală din ceea ce pare un container de 1,2x1,8x1,2 metri (lăţime x adâncime x înălţime). De fapt, chiar ESTE un container. Proiectilele sunt scoase din fabrica în acest container sigilat. Fiecare astfel de container are 15 proiectile şi poate fi transportat în spatele unui camion sau vehicul de teren Humvee. Odată ce conectezi un container PAM la câmpul de luptă wireless al internetului, proiectilele sunt

gata de lansare. În funcţie de câte ţinte inamice sunt estimate, ofiţerilor le sunt desemnate anumite zone ale câmpului de luptă şi li se dau parole pentru containerele PAM din acea zonă. Aceşti ţipi devin „experţii proiectilelor” şi sunt autorizaţi să trimită unul sau mai multe PAM-uri împotriva oricărui vehicul inamic care apare pe ecranul lor (care poate fi orice, de la un „Laptop de război” învechit la un ecran plat mai mare situat într-un cort al cartierului general sau într-un buncăr). Câmpul de luptă al internetului foloseşte aeronave, UAV-uri, sateliţi şi senzori tereştri pentru a alege ţinte. Atunci când expertul proiectilelor vede o ţintă pe care vrea să o distrugă, doar o indicaţie şi un click vor trimite coordonatele ţintei la un container PAM din apropiere, va lansa PAM-ul către o locaţie aproximativă, unde senzorii proiectilului vor alege ţinta, şi se va îndrepta spre ea. De cele mai multe ori, senzorii vor declara ţinta distrusă şi vor ajusta ecranul expertului proiectilelor în consecinţă.

Admiţând faptul că vor fi situaţii, precum cele în care ţintele sunt situate în păduri şi jungle, care vor împiedica senzorii să găsească prea multe ţinte, există un al doilea proiectil, LAM-u3 (Loitering Attack Missile), care are aceeaşi greutate ca şi PAM-ul, numai că este un proiectil care va zbura pentru aproximativ 45 de minute în căutarea unei ţinte. Dacă nu este găsită niciuna, se prăbuşeşte pur şi simplu şi explodează. Dacă este detectată o ţintă cu un radar încorporat (radar cu laser, sau LADAR, de fapt) şi software-ul încorporat recunoaşte vehiculul ca fiind unul inamic, proiectilul atacă de sus. Cu toate că focosul LAM-ul, şi nu este suficient de puternic pentru a distruge cea mai mare parte a tancurilor, orice altceva va fi probabil distrus prin ardere.

Elementele majore ale acestui sistem au fost deja testate şi toată chestiunea va fi probată în 2003. Nimeni nu îşi face iluzii că versiunea 1.0 a NetFires va funcţiona atât de bine. Atât de multe lucruri pot merge prost cu

identificarea ţintelor, siguranţa proiectilelor şi chiar câmpul de luptă al internetului. Odată ce vor fi rezolvate toate aceste probleme (probabil la versiunea 3.0), tot va trebui să îţi faci griji în legătură cu ce va face inamicul pentru a se apăra împotriva NetFires. Dat fiind gradul mare de dependenţă de comunicaţiile wireless, NetFires va trebui să îşi facă griji să nu fie atacat, bruiat sau în general dat peste cap. Când aduci internetul pe câmpul de luptă, trebuie să te aştepţi că vor fi şi hackeri acolo.

CAPITOLUL 10
DUŞMANUL: HACKERI BLACK HAT, SCRIPT KIDDIES ŞI CRACKERI

TERMENI TEHNICI

Glosarul complet, ce include şi termenii definiţi mai jos, poate fi găsit la sfârşitul cărţii.

Software de securitate – programe care scad şansele computerului tău de a fi avariat de atacurile de pe internet (viruşi, în mod special). Cel mai comun software de securitate este software-ul antivirus (care monitorizează PC-ul cu privire la prezenţa viruşilor şi îi elimina pe cei găsiţi) şi software-ul firewall (care blochează accesul oricărui element dăunător în PC).

Există cel puţin 30 de reviste şi aproape 500 de buletine de ştiri, mii de spaţii pentru chat şi câteva sute de mii de site-uri dedicate crackerilor, hackingului de tip black hat şi tot felul de comportamente frauduloase pe internet. Numele câtorva din aceste site-uri spun destul de clar ce se petrece acolo: hackers.com, securityfocus.com, rootshell.com, insecure.com, piracy.com şi tăticul tuturor: 2600.com. Dar chiar şi cu tot acest ajutor, numai aproximativ zece la sută dintre hackerii autodidacţi ştiu cu adevărat ce fac. Restul pur şi simplu descarcă instrumente de hacking şi merg să se joace cu ele pe web. Rezultatul sunt cele peste un milion de infracţiuni de pe net în fiecare an, plus multe milioane de alte încercări de acţiuni ilegale pe internet. Dacă eşti vreodată păcălit de vreunul dintre aceşti infractori, este foarte posibil să fie vorba despre vreun adolescent antisocial care a găsit instrumente infracţionale şi susţinere pe net.

HACKERI BLACK HAT

Hackerii black hat, profesioniştii în computere cărora

le place să producă pagube importante pe internet, nu sunt un grup prea mare. Sunt băieţi buni care, dintr-o serie de motive, au întrecut măsura şi şi-au folosit abilităţile pentru a produce pagube utilizatorilor de internet. Un motiv pentru înclinaţiile nestăpânite ale acestor persoane poate fi chiar natura internetului.

Internetul (şi mai ales World Wide Web) a devenit un instrument extrem de util pentru mulţi oameni, inclusiv pentru armată. Deşi este dat în folosinţă încă din 1969, acesta s-a răspândit rapid atunci când a devenit o operaţiune comercială în 1991 şi chiar şi-a luat zborul câţiva ani mai târziu când a apărut World Wide Web. Din păcate, simplitatea şi eficacitatea internetului a fost obţinută prin folosirea mai multor instrumente şi tehnici puse cap la cap de voluntari într-o atmosferă deschisă şi bazată pe încredere. Cu toate acestea, cu cât mai mulţi oameni au intrat pe net, cu atât a devenit mai normal să nu ai încredere în nimeni. Dar fapta fusese deja făcută, software-ul de care era nevoie pentru funcţionarea internetului nu mai putea fi retras şi protejat cu o mulţime de funcţii de securitate. Şi astfel avem un număr tot mai mare de hackeri (oameni care plănuiesc să ajungă acolo unde nu ar trebui să se afle) şi crackeri (aceia care o fac cu rele intenţii) care fac viaţa tristă (sau mai rău) utilizatorilor de internet.

Vulnerabilitatea de bază a internetului sunt numeroasele portiţe care permit informaţiei să pătrundă pe un server sau să iasă de pe el (un PC care face paginile web disponibile internetului). Gândeşte-te la „portiţe” ca la nişte linii separate de telefon deschise de către PC-ul tău pentru a permite unor sarcini diferite să fie îndeplinite simultan pe internet. Această capacitate este cea care îţi dă voie să descarci un fişier în timp ce mergi de pe o pagină web pe alta. În funcţie de cât de puternic este PC-ul tău, poţi descărca mai mult de o duzină de fişiere o dată în timp ce urmăreşti două sau trei pagini web. Fiecare locaţie

de internet (sau pagină de pe World Wide Web) rulează pe un computer (numit server) care este în permanenţă ataşat la internet printr-o conexiune telefonică. Internetul funcţionează pentru că orice utilizator poate găsi rapid o pagină web, un fişier de descărcat, sau orice altceva. O mare parte din lucrurile pretenţioase pe care le poţi face pe web (cumpărături, jocuri sau admirarea unor grafice pe o pagină web) implică programe de pe serverul care permite toate acestea, sau deschid serverul pentru intrări ilegale pentru aceia care ştiu cum funcţionează noul software. De multe ori există mai multe programe diferite care rulează pe server pentru a susţine o pagină web şi oricare din aceste programe poate avea o deschidere (port) intenţionată sau neintenţionată pentru un utilizator web care pătrunde în server. Aceasta este acţiunea de hacking (sau cracking).

În perioada de început a webului, hackingul era un sport inofensiv. Dar crackeri mai puţin cinstiţi (cunoscuţi şi cu numele de „hackeri black hat”) ştiu că odată intraţi pe un server, de multe ori pot prelua controlul şi pot face tot felul de înşelătorii. Mai sunt şi alte reţele în afara internetului, care pot fi sparte, dar este mult mai greu. Nicio reţea nu este perfecta, astfel încât nimeni nu este complet invulnerabil la atacuri. Dar unii sunt foarte bine protejaţi. Acest nivel de securitate are nevoie însă de timp, bani şi talent pentru a fi implementat şi niciodată nu sunt suficient de multe astfel de elemente, mai ales în organizaţii mari precum Departamentul Apărării. Un server bine protejat consumă de obicei prea mult timp pentru ca un utilizator legal să intre şi să îl folosească. În timpul anilor ’90 a avut loc dezvoltarea a două tipuri diferite de securitate pe internet. Marile organizaţii şi utilizatorii bine pregătiţi au servere bine apărate şi PC-uri apte pentru internet. Dar majoritatea utilizatorilor şi cele mai multe site-uri web nu sunt la fel de bine protejate. Acele site-uri securizate sunt atacate de cei mai pricepuţi

hackeri black hat din ambiţie sau pentru că ceva aflat pe server merită efortul de a fi furat. Site-urile şi utilizatorii mai puţin securizaţi sunt loviţi atât de hackeri talentaţi (pentru practică, pentru un câştig uşor, plictiseală etc.), cât şi de milioanele de amatori (care nu lasă nicio amprentă vizibilă pe site-urile mai bine protejate).

Hackerii black hat au creat un arsenal în plină dezvoltare de arme ce pot fi folosite împotriva site-urilor militare şi comerciale. Cu cât atacurile sunt mai ameninţătoare, cu atât sunt şi apărările mai îndârjite:

Atacurile DDOS (Distributed Denial of Service) întrerup serviciul de pe o reţea locală. Serverele web din sediile militare şi organizaţii au grijă de toate e-mailurile care intră şi care ies. Un atac DDOS va inunda serverul cu atât de multe mesaje, încât serverul nu va putea face nimic altceva decât să încerce să înfrunte invazia. Din 1999, există multe softwareuri care protejează serverele de atacurile DDOS, dar în 1999 nu prea existau multe astfel de atacuri şi nici prea multe software-uri noi care să le facă faţă. Aşa că la început armata a creat linii separate şi mai bine protejate pentru cea mai mare parte a mesajelor critice (cam cinci la sută din total).

Cu această abordare, traficul noncritic putea fi sigur, dar problemele adevărate rămân. În cele din urmă au fost instalate software-uri capabile să detecteze rapid şi să respingă atacurile DDOS pe site-urile care îşi puteau permite investiţia. Dar Departamentul Apărării este îngrijorat de gradul de complexitate tot mai mare al acestor atacuri. S-a observat că cineva a analizat cu atenţie Departamentul Apărării şi site-urile comerciale. Mai mult, acum există atacuri DDOS care atacă părţi diferite ale site-urilor mari cu diferite tipuri de arme DDOS. Cu această abordare, este posibil să ataci un site din direcţii diferite şi să eviţi măsurile de siguranţă, iar site-ul să nu mai poată funcţiona timp de mai multe zile. De asemenea, a fost descoperit recent că ruterele (PC-urile

specializate care direcţionează traficul pe net) pot fi şi ele atacate. Multe mecanisme de protecţie împotriva atacurilor DDOS se bazează pe ajustarea ruterelor pentru a devia cantităţile masive de atacuri DDOS asupra unui site. Cum dezvoltarea acestor forme mai sofisticate de atacuri necesită mai mult timp şi efort, se crede că unele guverne au angajat hackeri black hat pentru a crea o astfel de armă. Aşadar, deşi DDOS nu mai este arma înfricoşătoare care era în 1999, reprezintă încă o ameninţare dacă este utilizat de programatori bine instruiţi care ştiu ce fac.

Programele „Vampir” precum viermele Morris din anii ’80 erau încă văzute ca o ameninţare. Un program „Vampir” pătrunde în serverul tău şi face două lucruri. În primul rând începe să funcţioneze. De fapt nu face nimic, doar consumă din energia de procesare. Apoi „Vampirul” începe să se înmulţească. În scurt timp (câteva minute) serverul tău va fi atât de ocupat să ruleze sutele de copii de „Vampir” încât nu va mai putea face altceva. De asemenea, unele programe de felul acesta încearcă să folosească capacităţile de e-mail ale serverului pentru a se trimite către alte servere. „Vampirii” sunt într-adevăr o ameninţare întrucât pe software-ul de internet sunt găsite tot mai multe erori care oferă mai multe oportunităţi pentru ca un „Vampir” să se instaleze pe sistemele vulnerabile. Suspendarea de genul acesta în cazul unui server militar ar însemna viaţa sau moartea pentru trupele care depind de acel server pentru informaţii sau alte servicii. Armata a venit cu mai multe soluţii anti „Vampir”. Acestea includeau schimbări ale sistemului de operare care prevenea rularea în acelaşi timp a mai mult de câteva copii ale aceluiaşi program şi limita puterea de procesare pe care o folosea un program. De asemenea au fost instalate sisteme de detectare care căutau tipare ce indicau prezenţa unui „Vampir”. O mare parte din aceste idei de protecţie au fost acum incluse în software-urile de

securitate nou apărute. Dar armata nu poate aştepta ca sectorul comercial să le producă şi a încercat să rezolve această problemă. Acesta este un motiv pentru care Departamentul Apărării cheltuieşte mai mult de 20 de miliarde de dolari pe an pentru sisteme informatice.

Un tip comun de atac al hackerilor este a te strecura pe un server militar şi că copiezi fişiere pentru a le face publice. Uneori hackerii nu încearcă decât să puncteze politic prin dezvăluirea secretelor Departamentului Apărării. Hackerii black hat de acest fel sunt numiţi în mod obişnuit „hacktivişti”. Sunt şi situaţii în care fişierele nu sunt făcute publice, dar îşi fac drum către un guvern inamic. Cea mai bună soluţie găsită până în prezent a fost lăsarea unui număr mare de „ispite” aparent suculente, dar în realitate fără nicio valoare pe care hackerii să le găsească cu uşurinţă. Adevăratele bunătăţi sunt făcute să pară că nu merită deranjul. Conceput a fost extins la instalarea serverelor „Honey Pot” pentru a atrage hackerii. Aceste Honey Pot-uri sunt echipate cu software de detectare a intruziunii şi identificare pentru a ajuta la prinderea hackerilor.

— O altă metodă din anii ’80 este un program care pătrunde pe un sistem, caută o foaie de lucru şi fişiere de date după care schimbă cifrele aleatoriu. Apoi programul se autodistruge şi dispare orice urmă a lui. Este un tip de hacking foarte meschin pentru că poate trece ceva vreme până când îţi dai seama că datele au fost corupte. Până atunci este posibil să nu mai ai nicio copie bună rămasă (fişierele corupte au fost copiate de mai multe ori peste copiile bune). Este destul de dăunător pentru o companie, care poate pierde foarte mulţi bani în urma unui astfel de atac. Dar în cazul fişierelor militare, oameni pot muri. Singura apărare în faţa unui astfel de atac, pe lângă prevenirea lui înainte de toate, este un software care generează o sumă de control fun număr unic creat din datele din fişier) şi o înmagazinează într-un alt fişier.

Înainte să fie făcute copii de rezervă (o dată pe zi sau de mai multe ori), noi sume de control sunt generate şi comparate cu cele stocate. Sistemul va ignora fişierele care sunt editate (astfel de editări pot fi confirmate prin verificarea prezenţei recente a vreunui utilizator autorizat care să le fi făcut), dar se va aştepta la aceeaşi sumă de control pentru multele fişiere care nu sunt schimbate în fiecare zi. Dacă vreuna din aceste sume este diferită, administratorul de sistem este alertat şi pagubele produse pot fi reparate prin folosirea copiilor de rezervă bune. Dar, vai! sistemul sumelor de control este rar folosit în primul rând pentru că nu sunt mulţi hackeri black hat atât de meschini, încât să folosească un astfel de program. Dar ideea şi tehnicile există pentru a ţine acest tip de atac la mare circulaţie. Mai mult, un hacker black hat foarte talentat poate trece de protecţia sumei de control (asigurându-se că schimbările făcute sunt de aşa natură încât să nu modifice suma de control). De partea apărării, sistemele de operare recente au venit cu o criptare încorporată pentru documentele şi fişierele selectate. Chiar şi un black hat cu adevărat dedicat ar avea bătăi de cap cu schimbarea secretă a datelor din documentele codate.

Un alt tip de spargere ce dă coşmaruri sistemelor militare este acela care lasă un port deschis în server. Acest lucru îi permite să se întoarcă cu uşurinţă pentru a face ce doreşte. Poţi face asta prin spargerea unui computer şi lăsând un mic program care îţi oferă acces uşor şi nedepistat la server oricând vei dori în viitor. Această tehnică ar putea fi folosită dacă un guvern inamic ar plănui un atac de tipul celui de la Pearl Harbor. Dacă o mare parte din serverele americane ar putea fi atacate astfel, ar putea fi produse pagube foarte mari într-o scurtă perioadă de timp odată ce încep ostilităţile. Cea mai bună apărare împotriva acestor atacuri este monitorizarea constantă a serverelor în căutarea activităţilor neobişnuite

legate de porturile de comunicare care ar putea indica existenţa unui astfel de atac.

Un atac informaţional asemănător celui anterior este unul care sta pe un server şi activează (de obicei cu rezultate distructive) la o anumită dată sau când au loc pe server anumite evenimente (precum o activitate care să indice performanţa unei funcţii vitale, ca pregătirea pentru o operaţiune militară majoră). O cale de apărare este copierea periodic a tuturor informaţiilor de pe site şi apoi schimbarea datelor sau a tiparelor de rulare care ar putea atrage atacul. Nu este o soluţie grozavă, dar pentru cei cu adevărat paranoici sau pentru administratorii de reţea extrem de precauţi va fi suficientă.

După cum putem vedea din aceste tehnici, comunitatea hackerilor black hat (chiar formează una, mulţi dintre ei comunicând unii cu alţii) este cu siguranţă foarte talentată. Hackerii black hat care au revenit pe drumul cel bun subliniază şi ei că ceea ce îi motivează cel mai mult este atitudinea „poţi să faci asta mai bine?” şi dorinţa de a se lăuda cu abilităţile tehnici fără a fi constrânşi de restricţii morale.

TIPARE DE ATAC

Riptech, o companie de securitate pentru computere cu 300 de clienţi în 25 de ţări, păstrează înregistrările tuturor activităţilor de pe reţelele clienţilor (printre multe alte servicii de securitate). Este o măsură de securitate destul de comună. Deşi Riptech nu acoperă o mare parte din activitatea de pe internet, monitorizează un segment reprezentativ. A publicat un studiu despre 128.000 de atacuri care au avut loc în 5, 5 miliarde de înregistrări în ultimele şase luni ale anului 2001. În primele şase luni ale anului a avut loc o creştere de 80%.

Deloc surprinzător, 30% dintre atacuri au venit din SUA. Nu este surprinzător pentru că aceasta este ţara cu cea mai mare concentraţie de servere şi utilizatori de

internet. Dar SUA au furnizat numai 3, 5 atacuri la 10.000 de utilizatori web. Cea mai mare proporţie a atacurilor a venit din partea Israelului, cu 26 de atacuri la 10.000 de utilizatori. În ceea ce priveşte originea atacurilor, SUA au fost urmate de Coreea de Sud, China, Germania, Franţa, Canada, Taiwan, Italia, Marea Britanie şi Japonia. Cele mai multe dintre atacuri au fost de calitate inferioară, dar 43 % din clienţii Riptech au raportat cel puţin un atac serios. Cele mai multe din acestea păreau să fie făcute la întâmplare, dar 39% au fost deliberate. Viruşii Code Red şi Nimba au reprezentat 63% din toate atacurile, dar au fost excluşi din studiu pentru că ar fi trucat rezultatele. Companiile publice sunt de două ori mai expuse riscului de a fi atacate decât organizaţiile private sau nonprofit.

HACKERI BLACK HAT ŞI HONEY POT-URI

Spre deosebire de reţelele comerciale anterioare, internetul este folosit la scară largă. Un utilizator maliţios şi bine pregătit poate merge oriunde şi poate face multe înşelătorii; chiar şi distruge întreaga reţea. Navigarea în spaţiul cibernetic, monitorizarea şi vandalizarea site-urilor a devenit un sport de practicat. Există „o mişcare underground black hat (hacker)” ce îşi doreşte să ajungă în locuri unde nu ar trebui să fie şi unde fac ce le pofteşte inima. Hackerii white hat au fost depăşiţi numeric şi înfrânţi. Dar acest lucru se schimbă. Puţin.

Cel mai mare avantaj pe care îl au hackerii black hat este doar cel numeric. Există mai multe milioane de „script kiddies” care folosesc instrumentele de hacking pentru a desfăşura operaţiuni nocive pe web. O fac doar de dragul distracţiei, în acelaşi spirit care motivează mulţi adolescenţi puşi pe şotii. Dar script kiddies găsesc vandalismul pe internet mult mai distractiv pentru că pagubele sunt făcute la un nivel mai mare, şansele de a fi prinşi sunt mai mici şi nu este nevoie să te confrunţi faţă-n faţa cu victimele. Cea mai mare parte a comunicării se

desfăşoară în chat room, unde poate fi tolerat jocul preferat al adolescenţilor, acela de a te da drept altcineva. Nici măcar nu trebuie să fii foarte inteligent. Termenul de

„Script kiddies” provine din uşurinţa cu care instrumentele create de hackerii black hat sunt utilizate şi puse la dispoziţia oricui pe internet. Aceste instrumente nu necesită de obicei mai mult de o indicaţie şi un click şi furnizează scripturi uşor de folosit pentru hackerii black hat în devenire.

Înşişi hackerii black hat sunt mult mai puţini, numai câteva mii (sau numai câteva sute dacă îi pui la socoteală numai pe cei cu adevărat talentaţi care au trecut de partea întunecată). Cei mai mulţi dintre script kiddies au sub 18 ani şi astfel e puţin probabil să fie prinşi şi închişi. Dar hackerii white hat care se plictisesc de vreun script kiddie care merită efortul de a fi urmărit, descoperă că un singur apel telefonic către părinţii acestuia de multe ori dă rezultate. Hackerii black hat preferă să rămână în continuare anonimi pentru că sunt suficient de mari pentru a fi arestaţi şi condamnaţi. Şi o mare parte dintre ei chiar sunt.

Dar cei mai îngrijorători hackeri black hat sunt adevăraţii infractori. Unu dintre aceştia lucrează pentru guverne şi îşi folosesc abilităţile pentru spionaj şi furt de tehnologie. Aceştia sunt cei care lucrează pentru bani.

Comunitatea underground a infractorilor internetului deţine o mulţime de informaţii. Sfaturi tehnice şi vulnerabilităţi ale internetului, toate sunt oferite la schimb prin intermediul unor chaturi protejate de parolă şi pe grupurile de e-mail codate. Script kiddies joacă un rol major în furnizarea unei mari părţi din aceste informaţii. Numerele contează şi ei au timp berechet să cutreiere internetul şi făcând mişcări periculoase pe care hackerii black hat mai în vârstă le evită. Copiilor le place să se laude şi hackerii black hat ascultă şi iau notiţe despre noile modalităţi de protecţie descoperite de script kiddies.

Atunci când hackerii black hat văd o nouă vulnerabilitate promiţătoare, operează singuri. Sunt foarte precauţi. Infractorii black hat îşi planifică operaţiunile cu la fel de mult profesionalism ca un jaf armat. Nimic nu este lăsat la voia întâmplării, întrucât dacă eşti prins îţi poate fi fatal (în China, hackerii black hat prinşi comiţând infracţiuni sunt uneori ucişi). Un hacker black hat talentat îşi va observa ţinta cu atenţie şi în mod sistematic pentru a-i afla slăbiciunile şi metodele de protecţie. Acest proces se poate întinde pe mai multe zile sau săptămâni cu pauze pentru a cerceta metodele de protecţie necunoscute sau o posibilă slăbiciune din software-ul site-ului. Atunci când reuşeşte să intre pe site, hackerul black hat va lua informaţiile şi va pleca. O mai mare perioadă de timp va fi acordată studierii celor găsite. În cele din urmă, după sute de ore de muncă, hackerul black hat va face următoarea mişcare şi va fura ceva sau pur şi simplu va bloca site-ul.

Până de curând, singurul mod în care puteai afla despre o operaţiune de succes a unui hacker black hat era atunci când deja nu se mai putea face nimic. Şi uneori nici măcar atunci. Hackerii black hat îşi acopereau urmele cu atenţie. Pentru ei, o operaţiune de succes era una ce nu era descoperită niciodată. Principala metodă de a-ţi acoperi urmele este să găseşti înregistrările serverului, cu tot ce se întâmplă pe site (cine intră pe server şi ce face), şi să ştergi intrările care pot identifica pătrunderea prin efracţie. De multe ori este un lucru greu de făcut întrucât aceste înregistrări sunt adeseori codate sau protejate prin detectarea intruziunii sau printr-un software anti-falsificări. Dar este semnătura unui hacker black hat să nu lase nicio probă în urma sa.

Atunci hackerii white hat au venit cu termenul de Honey Pot.

Un Honey Pot este un server de internet (un PC pe care rulează un site web) care pare real, dar este monitorizat cu atenţie pentru a înregistra tot ce face

hackerul black hat. Astfel, hackerii white hat pot aduna informaţii despre hackerii black hat şi au mai multe şanse de a-i prinde. Din cauza costurilor mari şi a volumului mare de muncă, nu este practic să pui acest software de monitorizare pe fiecare site. Băncile şi serverele de înaltă securitate ale guvernelor au sisteme de protecţie care monitorizează fiecare (sau aproape fiecare) intruziune şi se opresc dacă este detectată vreo intrare neautorizată. Acest lucru nu ajută la identificarea hackerilor black hat, dar aceste site-uri nu vor decât să rămână în siguranţă şi nu să facă pe poliţiştii.

Honey Pot-urile s-au dovedit a fi instrumente utile pentru a afla ce fel de instrumente şi tehnici folosesc hackerii black hat. De exemplu, Honey Pot-urile pot arăta cum îşi acoperă hackerii black hat urmele (prin modificarea înregistrărilor sau alte trucuri de care nimeni nu a mai auzit până acum). Acest lucru ajută la construirea unei mai bune apărări. De asemenea, acestea îi deranjează pe hackerii black hat, făcându-i mai puţin încrezători atunci când se gândesc dacă nu cumva fiecare site pe care îl sparg este măsluit pentru a-i prinde. Odată ce s-a răspândit vestea că există Honey Pot-uri, hackerii black hat au fost nevoiţi să îşi petreacă mai mult timp încercând să afle dacă serverul pe care îl sparg este sau nu un Honey Pot. Acest lucru nu este tocmai uşor, ceea ce îi bucură pe hackerii white hat.

Cu toate acestea, hackerii black hat ştiu că există Honey Pot-uri şi ca războiul tehnologic abia a început. Hackerii white hat fac aceste Honey Pot-uri din ce în ce mai performante. Ca bonus, ei adaugă elemente serverelor non-Honey Pot pentru a-i face pe hackerii bine pregătiţi să creadă că este de fapt un server-capcană. Astfel, o parte din tipii răi sunt ţinuţi la distanţă. O sperietoare de ciori electronică, ca să spun aşa. Un bonus, cum ar veni.

Toate acestea nu se petrec în văzul lumii. Mii de administratori de servere au software ilegal instalat pe

sistem în urma unor acte de vandalism (mai ales respingerea serviciilor, sau atacuri DDOS). Guvernul american a detectat mai multe spargeri ale site-urilor militare şi furturi de informaţii. Ceea ce îi îngrijorează sunt spargerile pe care nu le-au descoperit. Deşi nu se aud multe lucruri despre asta, din motive evidente, Honey Pot a devenit o armă militară. Pe timp de război hackerii black hat militarizaţi ar putea distruge serverele Departamentului Apărării mai repede decât un proiectil. În acel moment, o parte dintre script kiddies şi-ar putea da seama că sunt posibili trădători. Dar până atunci, puştii vor doar să se distreze.

CYBER-CRIME ŞI CYBER-TERORISM

Odată ce lumea a părut că a supravieţuit spaimei Y2K relativ nevătămată, atenţia a fost îndreptată către alte modalităţi de a afecta funcţionarea unui PC. într-adevăr, unul dintre câştigurile verificărilor masive şi reprogramării proiectului Y2K (pentru a nu se prăbuşi programele pentru că anul era înregistrat cu două cifre, iar computerele să recunoască „00” drept 1900 în loc de 2000) a fost numărul masiv de erori găsite în programele de comunicare. Proiectul Y2K cerea ca o mare parte din software să fie monitorizată aşa cum nu mai fusese până să apară pericolul avariilor cauzate de Y2K. înainte de asta, atitudinea obişnuită la adresa unui software era „dacă nu e stricat, nu-l repara”. Dar multe software – un care păreau să funcţioneze bine aveau de fapt probleme ce nu aveau nicio legătură cu Y2K. Existau multe software-uri vechi de 30 de ani pe care puţini programatori le mai înţelegeau cu adevărat. Dacă ele cedau, era angajat un consultant scump care le repara, dar nimeni nu să obosit să pună pe cineva să verifice dacă există probleme mari care mustesc în interior. Din cauza miliardelor de dolari cheltuiţi pe rezolvarea problemelor Y2K, multele chestiuni ale software-urilor mai vechi au devenit cunoscute. Dintr-

odată, lucruri până atunci necunoscute au devenit importante. Acest fapt cumulat cu posibilitatea tot mai mare de atac asupra computerelor prin conexiuni la internet au făcut ca tot mai multe companii şi lideri guvernamentali să fie conştienţi de ameninţarea ignorată anterior.

Când lumea se pregătea de ieşirea din anii ’90, existau mulţi ciudaţi cu intenţii rele pe internet cărora le plăcea să exploateze erorile software-urilor de comunicaţii, să ajungă acolo unde nu ar trebui să meargă şi să facă lucruri pe care nu ar trebui să le facă. Organizaţiile guvernamentale şi militare erau preocupate cel mai mult de folosirea acestor atacuri ca armă militară. Unele naţiuni, în special SUA, cheltuiseră deja bani pentru cyber-război şi deveneau conştiente de unele vulnerabilităţi potenţiale majore. Oamenii îşi dădeau seama că există o ameninţare chiar cu arme nucleare, război chimic şi folosirea armelor biologice

— Departamentele poliţiei şi agenţiile secrete de informaţii au, de obicei, un grad ridicat de securitate în sediile lor centrale. Dar sunt multe „filiale” cu securitate slabă. Agenţiile secrete de informaţii lucrează de obicei cu departamentele de poliţie locale şi înregistrările electronice de aici sunt şi mai uşor de accesat. Genul acesta de infracţiune stârneşte foarte mult interesul organizaţiilor infracţionale şi hackingul se pare că şi-a găsit locul aici (să găsească numele martorilor oculari, dacă vreun gangster e investigat sau are microfoane amplasate).

— Un alt domeniu cu un impact militar şi multe beneficii pentru terorişti e spargerea şi subminarea sistemelor computerizate ale judecătoriilor şi închisorilor. Operaţiunile de acest fel prezintă deja un mare interes pentru bandele de infractori, care deseori îşi oferă serviciile oricui oferă suficienţi bani. Jocul cu sistemele computerizate ale judecătoriilor şi închisorilor face

posibila scoaterea oamenilor tăi de nivel mic şi mijlociu din închisoare (şi din ţară înainte să fie rearestaţi).

Sistemele computerizate ale imigrărilor şi vămii. Spargerea lor poate da voie sabotorilor şi spionilor să intre (sau să iasă) într-o ţară inamică mai uşor. Serviciile computerizate al vămii care au fost sparte pot lăsa să pătrundă contrabanda cu bombe şi tehnologie furată.

Sistemele de apărare aeriene sunt de mult timp computerizate. Statele Unite au făcut asta prima dată în 1950 (ce a dus la producţia şi crearea primelor modemuri). Spargerea acestor sisteme le poate pica sau poate da voie raporturilor false să apară pe ecranele radarelor inamice.

Sistemele controlului de trafic aerian sunt legate printr-o reţea, în mod ironic, cea mai bună apărare a sistemelor controlului de trafic aerian sunt computerele vechi care le rulează. Asta face şi mai dificil (dar nu imposibil) cyber-războinicilor sau teroriştilor să intre şi să comită infracţiuni (sau să intervină subtil în operaţiunile aeriene pentru a perturba operaţiunile de război). Computerele mai vechi nu au fost create să aibă acces la internet şi majoritatea hackerilor nu sunt familiarizaţi cu acestea. Sistemele controlului de trafic aerian militar, care folosesc computerele moderne, sunt mai bine protejate, dar tot vulnerabile.

— Un alt sistem de transport vulnerabil sunt căile maritime. E adevărat în privinţa acelor râuri şi canaluri ce depind de baraje ca să regleze nivelurile de apă pentru traficul sigur al bărcilor şi vapoarelor. Accesul la acele sisteme (cel puţin cele care au acces la internet) ar furniza o oportunitate de a provoca daune sistemelor de irigaţie şi de distribuţie a apei.

— Dispozitivele industriale (centrale electrice nucleare şi convenţionale, centrale chimice, rafinării sau alte dispozitive industriale) sunt vulnerabile dacă sunt modificate prin conectarea la internet. Asta ar cauza rănirea sau uciderea a mii de civili, ca să nu mai vorbim de

daunele sau distrugerea dispozitivelor.

De reţinut: multe dintre sistemele enumerate mai sus poate că au fost sparte cu succes deja, dar nu s-a observat pentru că există atât de multe probleme care sunt cu siguranţă (sau asta se crede) consecinţele erorilor umane. Majoritatea problemelor sistemelor computerizate s-au datorat întotdeauna erorilor umane (fie în crearea lor, fie în întreţinerea hardware-ului sau software-ului). Într-adevăr, au existat mai multe probleme cauzate de erori umane, comparativ cu spargerea evidentă a sistemelor, încât e foarte greu să găseşti un hacking bun printre toate problemele cauzate de prostia oamenilor.

CYBER-CRIMINALI

Activitatea infracţională pe internet creşte odată cu numărul operaţiunilor comerciale vulnerabile efectuate online. Au existat mereu tehnicieni care s-au dedat infracţiunilor şi s-au îmbogăţit (sau au fost închişi) folosindu-şi competenţele ilegal. Târziu în Războiul Rece, sovieticii au recrutat echipe de hackeri din Europa de Vest să spargă sistemele militare ale NATO şi cele guvernamentale. Informaţiile secrete erau ţinta lor şi cunoaştem doar infracţiunile pentru care hackerii au fost prinşi şi condamnaţi. Hackerii infractori în general sunt deschişi ofertelor oricui (pentru o sumă corectă) să facă orice.

Mai îngrijorător era numărul crescut de cyber-infractori ce operau în Rusia şi Europa de Est după Războiul Rece. Aceste grupuri aveau o mare îndemânare şi se orientau asupra băncilor şi alte site-uri bine protejate. Sunt trei motive principale pentru o asemenea concentrare de talent de hacking în acest domeniu. Primul era sistemul educaţional din era comunistă care producea mai mulţi ingineri şi oameni de ştiinţă decât locuri de muncă. Apoi, era de mult timp o lipsă a hardware-ului decent în ţările comuniste. Ce era disponibil tindea să fie o tehnologie

primitivă comparabil cu ce se găsea în Statele Unite, ce le cerea programatorilor de acolo să muncească mai mult cu mai puţin. Mai mult, naţiunile comuniste nu-şi permiteau să cumpere computere mai noi, mai bune şi mai puternice o dată la un an sau doi, aşa că programatorii trebuiau să folosească la maximum hardware-ul vechi şi limitat. Aceste economii socialiste sărace produceau mulţi programatori prost plătiţi cu competenţe excelente. Apoi, în timpul perioadei comuniste un programator talentat nu avea cum să creeze un nou produs şi să beneficieze de pe urma lui. Într-adevăr, se practica furtul, software-ul din Vest era văzut ca ceva ce putea fi furat, sau de luat

(ignorând copyrightul şi protecţiile patentate) pentru dezvoltarea de noi produse. A pârata software-ul altcuiva şi a-l folosi fără să ţii cont de drepturile intelectuale (sau de alt fel) a devenit o parte a culturii locale. Acest fenomen a produs şi competenţe superioare de hacking. În timp ce mulţi programatori din această regiune au revenit, mulţi au rămas de partea întunecată. Competenţele au devenit disponibile pentru operaţiuni infracţionale, militare sau teroriste pe internet şi Europa de Est a devenit paradisul cyber-infractorilor. Gangsterii mai convenţionali erau rapizi în învăţarea escrocheriilor pe internet. Unele din bandele de infractori din Europa de Est erau mai eficiente decât cele vestice şi ştiau cum să-şi motiveze hackerii prin teroare, sau cu bani. Iar preţul eşecului unei escrocherii era deseori moartea. Nu e genul de motivaţie predată de şcolile vestice de afaceri, dar este eficientă până la un punct.

La începutul secolului XXI, Rusia şi naţiunile est-europene, sub presiunea Americii şi a celorlalte naţiuni europene, au început să aresteze cyber-infractorii. Dar din cauza gradului de corupţie din Europa de Est (mai ales în Rusia), oficialii guvernamentali iau parte, uneori, la escrocherii. Ocazional, asta se făcea oficial, când hackerii erau plătiţi de guvern să facă spionaj militar şi industrial.

Cum mulţi dintre infractori sunt un fel de patrioţi, mai sunt alţii (ca multe bande cecene din Rusia) care lucrează cu teroriştii. Ca majoritatea infractorilor, hackerii se vând oricui. Pentru agenţiile antitero vestice, aceasta e o problemă mare când vine vorba de instrumente de codare ilegale vândute de hackerii din Europa de Est. Majoritatea naţiunilor determină ce fel de instrumente de codare pot fi vândute direct şi infractorii est-europeni au văzut în acest proces încă o escrocherie profitabilă (ca şi drogurile, prostituţia, şantajul şi aşa mai departe). Teroriştii, ca şi infractorii de rând, foloseau cele mai puternice sisteme de codare ca să-şi ţină comunicaţiile secrete.

E mult mai greu pentru infractori, totuşi, să obţină servicii de cyber-război ce pot răni conaţionalii hackerilor. De exemplu, doar câţiva hackeri europeni ar ajuta la spargerea sistemului controlului de trafic aerian, sau sistemului de comunicaţii al rachetelor nucleare în acele ţări. Dar pot deveni mercenari pe viitor. De exemplu, bandele cecene (musulmane şi câteodată pro-al-Qaeda) îşi dezvoltă propriile grupuri de hacking, deci o asemenea precizie ar putea să nu mai fie o problemă pe viitor.

Hackerii din Vest şi superputerile de software în dezvoltare precum India şi China furnizează suficiente locuri de muncă legitime şi profitabile (şi sigure) pentru cei ce ar fi tentaţi să încalce legea. Acest lucru s-a întâmplat mereu în Vest, când şi un hacker condamnat îşi poate găsi un loc de muncă bun după ce iese din închisoare. Totuşi, tentaţiile sunt mereu acolo. Mulţi programatori indieni şi chinezi îşi petrec mult timp liber învăţând complexitatea internetului. Aceasta duce mai întâi la manipulare din joacă. Apoi, deseori, duce, ca de multe ori înainte, la escrocherii (fraude cu carduri de credit, de obicei). Tinerii programatori tind să-şi dezvolte un simţ al invincibilităţii şi asta-i duce să încerce, şi câteodată să reuşească, un furt calificat pe internet. Acest fapt e înrăutăţit de ezitarea marilor companii financiare de

a raporta aceste furturi. Dar lucrurile se schimbă, iar companiile împreună cu, poliţia îşi dezvoltă competenţele în urmărirea şi prinderea cyber-infractorilor. Dar cel puţin pentru prima decadă a secolului XXI, economiile în plină dezvoltare din Europa de Est, şi mai ales Rusia, vor rămâne un teren propice pentru săvârşirea infracţiunilor pe internet.

SCHEME OBIŞNUITE DE FRAUDĂ PE INTERNET

Majoritatea infracţiunilor de pe internet sunt *low-tech.* Şi cele mai multe se fac prin email. Oricine foloseşte e-mailul ştie totul despre „spam" (mail nesolicitat) şi aşa acţionează cei mai mulţi infractori pe internet. În ciuda naturii *low-tech* a infracţiunilor, e important de ştiut acest aspect, pentru că şi escrocheriile *high-tech* exploatează natura umană. Amintiţi-vă, majoritatea intruziunilor ilegale în sistem se fac prin parolele furate.

Mai jos e o listă a celor mai des întâlnite infracţiuni pe internet. Dacă vei fi tentat să pici într-una din curse, n-o face. Acum vei şti mai bine.

Oportunităţile de afaceri (deseori un fel de ofertă „lucrează de acasă" cum ar fi introducerea de date sau răspunsul la e-mailuri pentru o firmă). Funcţionează prin afişarea unei oportunităţi atractive, cu nimic de pierdut, „fără obligaţii", Totuşi, se percepe o mică taxă administrativă. În zilele dinaintea apariţiei e-mailului, taxa era mai mare pentru a acoperi costurile reclamelor sau a expedierii prin poştă. Dar spamul nu necesită plicuri, timbre sau material printat şi e mult mai ieftin. Trimiterea spamurilor nu costă nimic. Asta le permite infractorilor să perceapă o „taxă de procesare" mai mică, ce sigur va fi plătită. Deseori cam de zece sau douăzeci de dolari, atât de mică. Hoţul scapă folosindu-se de viteza internetului. Trimite spamuri la milioane de oameni, adună banii la o căsuţă poştală (închiriată sub un nume fals), depune

cecurile (într-un cont deschis cu un act de identitate fals), le încasează şi dispare înainte ca cineva să se aştepte să primească serviciile promise. Aceşti infractori ştiu destule despre cum funcţionează internetul pentru a folosi IP-uri false. Singurii infractori care sunt prinşi făcând aceasta sunt amatorii care nu şi-au calculat timpul de acţiune şi stau destul de mult într-un loc ca să fie prinşi.

Furtul cardurilor de credit e în continuă creştere. Cele mai furate informaţii atunci când site-ul unor firme e spart sunt cele legate de cardurile de credit. Stai pe lângă **site-urile** hackerilor black hat şi ale unor script kiddâes şi curând vei avea acces la numerele cardurilor de credit furate (pentru o sumă sau pentru că cineva e generos). Folosirea plasticului furat poate fi înşelătoare, deoarece industria cardurilor de credit în valoare de trei miliarde de dolari îşi permite o tehnologie de ultimă oră şi talentul de a-i urmări pe aceşti escroci. Din nou, profesioniştii cu experienţă scapă şi tinerii amatori sunt prinşi din prima. Unu script kiddies caută un site de e-business cu informaţii despre cardurile de credit şi, pentru o perioadă în anii ’90, puteau trece de protecţia slabă sau neglijentă des întâlnită pe atunci pentru a fura informaţii despre cardurile de credit. În ziua de azi, pot ajunge într-un Honey Pot, urmat de o vizită a FBI (frauda cardurilor de credit este o infracţiune federală şi agenţilor le place să aresteze amatori ca o avertizare pentru ceilalţi).

— Cererea de informaţii oficiale. Această cerere falsă poate veni de la o companie sau de la o agenţie guvernamentală cu care destinatarul lucrează. O schemă întâlnită e să trimită spamuri clienţilor unui ISP (cum ar fi AOL sau Earthlink) cu cereri ciudate (dar care arată oficial) pentru informaţii despre noile carduri de credit. „… pentru că există o problemă cu prezentul card de credit”. După ani de zile de avertizări din partea ISP-urilor, oamenii tot cad pradă. Un spam fals trimis de guvern pretindea a fi de la Fisc şi cerea destinatarului să completeze un

chestionar în 48 de ore „altfel…”. Spamul cerea informaţii precum numerele de asigurare socială şi datele contului bancar. Acesta continuă să apară an de an în perioada de două luni de dinainte de plata impozitelor de pe 15 aprilie.

Fraudarea instituţiilor financiare e făcută doar de profesionişti. Hackerul trebuie să ştie cum funcţionează băncile şi instituţiile financiare. În multe din aceste organizaţii se obişnuieşte ca unele tranzacţii să fie autorizate printr-un e-mail de la o sursă cunoscută. Ca să-ţi reuşească, trebuie să afli cine poate fi înşelat să aprobe un împrumut, transfer bancar sau altceva. Genul acesta de lucruri poate uneori să implice un grup hacking puternic şi rareori spamul.

Frauda prin investiţii e un alt spam preferat. Cel mai întâlnit implică o persoană (expeditorul spamului) care caută un partener (victima) deţinător de cont bancar pentru a facilita mutarea ilegală (sau semilegală) a unor sume de bani dintr-un cont străin. Consecinţa e golirea contului tău bancar. O altă fraudă prin investiţii este vinderea la preţuri foarte mari a sistemelor de protecţie, sau a celor fantomă (false) pe internet. Acest gen de înşelăciune se făcea faţă în faţă, dar acum se face mult mai eficient pe internet. Ca întotdeauna, dacă vrei să faci ceva rapid şi eficient, foloseşte computerul.

Neonorarea comenzilor de bunuri şi servicii e de obicei consecinţa incompetenţei, nu a fraudei, dar rezultatul e acelaşi. Din nou, viteza internetului permite multor fraude ca aceasta să reuşească. Reclamele prin spamuri, deseori realizate cu îndemânare grafică HTML, sunt create să arate veridic. Aceste escrocherii deseori iau carduri de credit, care necesită mai multă mu**ncă din partea infractorilor (companiile de carduri de credit sunt atente la asemenea infracţiuni). Câteodată sunt oferite servicii, cum ar fi ajutor în luarea unei slujbe sau unui** împrumut. O variaţie pe internet a acestora a folosit licitaţiile online foarte populare. În ciuda eforturilor

neobosite, pe site-uri precum ebay, încă se fac fraude (oamenii vând lucruri pe care nu le au) în acest domeniu. Ca întotdeauna, cumpărătorule, ai grijă.

— Escrocheriile Ponzi (sau piramidale) au o nouă viaţă pe internet. Oamenii sunt convinşi să investească în ceva foarte sigur (schimb valutar, ipoteci ale caselor din străinătate sau mai ştiu eu ce) şi primii investitori primesc sume generoase după aceasta. Însă oamenii din spatele escrocheriei nu investesc bani. Plătesc unele din sumele investite ca „dividende" ca să creeze cerere şi să aducă mai mulţi investitori. Când li se pare, hoţilor, că valul noilor investiţii a crescut, dispar cu banii. E o înşelătorie veche, faimoasă prin anii '20, creată de un domn Charles Ponzi, căruia i-a reuşit o escrocherie spectaculoasă de genul acesta, după Primul Război Mondial.

ANUL DDOS

În vara anului 1999, au avut loc primele atacuri DDOS. DDOS, sau atacurile Distributed Denial of Service, profită de punctele slabe din protecţia software-ului de internet. Multe din comenzile de bază pe care internetul le foloseşte pentru ca serverele să comunice între ele pot fi falsificate cu uşurinţă (sau „înşelate"). Prin trimiterea de comenzi înşelătoare câtorva servere, le poţi păcăli să trimită o cantitate imensă de mesaje de control unui anumit server. Indiferent de capacitatea unui server (sau, câteodată, a unui grup de servere), dacă-i trimiţi destule comenzi de control, îl poţi închide. Ei, nu-l poţi chiar închide, dar serverul ajunge să se ocupe doar de mesajele false şi nu mai are timp să facă altceva. Cam ce se întâmplă când prea mulţi oameni se loghează pe site-ul Victoria's Secret să vadă prezentarea lenjeriei. Ce a fost unic la atacurile DDOS din 1999 a fost utilizarea de programe zombie: programe postate în secret pe sute de servere ca să lanseze un atac DDOS şi mai intens. Atacul din 1999 asupra serverului unei universităţi a blocat

website-ul acesteia pentru două zile folosind o armată de 227 programe zombie.

În primul rând, hackerii black hat chiar treceau de partea întunecată pentru a reuşi acest timp de atac. Era nevoie de ceva efort să creeze programul zombie şi să-l distribuie. De fapt, hackerii aveau propria mişcare răufăcătoare *Open Source,* păstrând chiar şi programul zombie, iar cel folosit în 1999 era primul dintr-o serie ce a fost constant reparată şi „îmbunătăţită" până acum. Viziunea *Open Source* era destul de înfricoşătoare, pentru că însemna că zeci (dacă nu sute) de programatori cooperau pe ascuns pe internet pentru a crea instrumente de atac asupra internetului.

În al doilea rând, erau două motive pentru dezvoltarea programelor zombie. Cel mai evident dintre ele era că puteai genera un flux mai mare de date şi astfel să închizi site-uri mai complexe. Dar programele zombie făceau şi mai greu de prins vinovatul. Cu vechile tehnici, trimiterea de mesaje de control dintr-un loc însemna că trebuia să stai online cât făceai asta. Aşa că un hacker deştept şi muncitor te putea prinde în flagrant. Nu aveai un aşa noroc cu programele zombie, decât dacă prindeai hackerul în timp ce instala unul din programe.

În alt treilea rând, erau atât de multe servere prost supravegheate pe care hackerii black hat puteau instala mii de programe zombie. Odată ce făceau asta, puteau lansa atacuri DDOS capabile să blocheze orice site-uri mari de pe internet. În timp ce hackerii white hat şi multe firme de software lucrau din greu să dezvolte instrumente pentru stoparea atacurilor DDOS, treceau luni de zile până ca acestea să apară, şi ani înainte ca programele anti-DDOS să fie disponibile pe internet. De fapt, s-a întâmplat să apară un fel de cursă a înarmărilor, cu programatorii răuvoitori DDOS ce veneau cu un nou software de atac, pe cât de repede companiile de protecţie pe internet puteau dezvolta noi programe de apărare împotriva DDOS.

În al patrulea rând, şi ce e mai şocant pentru FBI, se pare că exista o vastă reţea underground de hackeri black hat despre care nu ştiau. Ups.

Pe 7 februarie 2000, a mai picat o bombă. Un masiv atac DDOS a lovit cel mai popular site web, yahoo.com, făcându-l indisponibil pentru câteva ore. În următoarele zile, au mai fost atacuri DDOS similare pe site-uri mari precum Amazon.com, CNN.com. ETrade şi ebay. Până pe 9 februarie 2000, internetului, îngreunat de traficul suplimentar al atacurilor DDOS, îi luă 26% mai mult (pe medie) să ruleze o aplicaţie (cum ar fi să încarce o pagină web sau să downloadeze un document).

Un elev canadian de 15 ani a fost prins şi acuzat de lansarea atacurilor DDOS. Deşi era responsabil pentru unele din ele (şi a pledat vinovat la începutul lui 2001, fiind prins pentru că se lăudase), investigaţiile ulterioare au arătat că au fost mii de script kiddies şi hackeri black hat care aveau acces la instrumente DDOS şi au ştiut cum să le folosească. Până spre finalul anului 2001 au fost estimate unul sau două atacuri DDOS pe săptămână asupra marilor site-uri, şi mai multe asupra celor mici. Marea majoritate erau o pierdere majoră de timp pentru succesul site-ului. Dar, cu excepţia câtorva atacuri, cum ar fi cel asupra Microsoft de la începutul lui 2001, nu a existat un holocaust DDOS. De fapt, la cât de dese erau atacurile DDOS, loveau cam un website din 10.000 săptămânal. Nu doar atât, dar durata medie a unui atac DDOS era de zece minute. Se auzea doar de atacurile care închideau site-urile zile întregi (sau, cel puţin într-un caz, definitiv).

Se vorbea în cercul hackerilor black hat (legea monitoriza acum unele din conversaţiile lor „secrete”) de închiderea accesului la internet într-o întreagă ţară (cum ar fi China sau Egipt) prin atacuri DDOS. Se menţionau şi atacuri plănuite cu grijă asupra ruterelor-cheie, de a încerca şi bloca accesul la internet în părţi ale Statelor

Unite sau a marilor website-uri. Ameninţările erau credibile, căci era acum disponibil un număr de alte programe zombie şi multe tipuri de atacuri ce puteau fi duse la bun sfârşit.

Se pare că o mare constrângere pentru problemele DDOS era conştientizarea în cercul hackerilor black hat că erau mulţi poliţişti pe urmele lor. Numai FBI avea şase investigaţii în desfăşurare la începutul anului 2001. Poate cel mai înfricoşător lucru era numărul de hackeri white hat foarte capabili care căutau peste tot. Singurul lucru de care hackerii black hat şi script kiddies se temeau era un hacker white hat nebun – care era şi bun. Aşa au fost prinşi, condamnaţi şi trimişi la închisoare majoritatea hackerilor black hat.

Unul din lucrurile despre care nu se vorbeşte în comunitatea hackerilor black hat e că, atunci când vine vorba de cantitatea şi calitatea îndemânărilor de hacker, hackerii white hat au un avantaj considerabil. Pur şi simplu sunt mai mulţi hackeri white hat şi cei mai buni hackeri de internet tind să fie cei white hat (sau, în cel mai rău caz, hacker gray hat, oameni care au fost răuvoitori în trecut, dar s-au îndreptat). Hackerii black hat sunt toleraţi cât timp nu-i supără pe hackerii white hat prea mult. Dar dacă-i enervezi rău de tot pe unii hackeri white hat, vor veni după tine. Şi de cele mai multe ori, te vor prinde. Dacă eşti norocos, doar te vor umili şi da la o parte. Dacă eşti deştept, vei sta pe loc şi vei înghiţi jignirea cât se poate de graţios. Căci alternativă e o vizită a FBI. Unii hackeri white hat vor să prindă un hacker black hat enervant, dar nu vor să-şi piardă timpul ajutând FBI-ul. Aşa că cel mai frică hackerilor black hat le e de un hacker white hat cu mult timp la dispoziţie.

Atacurile DDOS asupra Yahoo de la începutul anului 2001 au fost cele care au introdus guvernul Statelor Unite în războiul cibernetic, înainte de aceasta, FBI dobândea încetul cu încetul expertiză în IT şi protecţia internetului,

dar şi o mai bună înţelegere a ceea ce însemna de fapt hackingul. În mod normal, FBI trata infracţiunile IT la fel ca pe orice altă formă de infracţionalitate. Adică, cazurile mari interstatale (ca să devină problemă federală) captau atenţia FBI. Toate celelalte erau transferate poliţiei locale. Dar asta era o mare parte a problemei FBI. Când era vorba de internet, nu era, oricât de mult ne-am gândi, un caz local. Şi cele mai multe departamente ale poliţiei locale (incluzând poliţia statală) erau la fel de nepregătite în ceea ce priveşte problemele de IT şi protecţia internetului pe cât era şi FBI. Chiar şi denunţarea unei infracţiuni pe internet era dificilă. Mulţi oameni au mers la poliţia locală. În majoritatea cazurilor, poliţia ştia că era un caz federal. Dar, curând, CIA trecea majoritatea cazurilor procurorului general sau doar spunea (cu aşa multe cuvinte) că nu se putea ocupa de aceste cazuri. Mult timp în anii ’90, FBI se străduia să-şi dea seama cum să se descurce cu avalanşa de infracţiuni pe internet. Între timp, companiile, sau indivizii bogaţi, trebuiau să plătească investigarea acestor infracţiuni. Procurorul general din regiune trebuia să facă acuzaţii dacă părea un caz ce se poate câştiga. Abia în ultimii am lucrurile au început să se schimbe, căci FBI, fiscul şi întregul sistem federal de justiţie a deschis birouri unde victimele pot denunţa infracţiuni pe internet, iar anchetatorii pot urmări infractorii cibernetici.

Totuşi, existau agenţii federale care aveau cunoştinţe despre reţea. Fundaţia Naţională de Ştiinţă (NSF), care se ocupa cu tranziţia de la ARPANET la internet, ştia totul despre reţea. Dar nu exista o agenţie a poliţiei. De asemenea, CIA şi micul sau frate secret, ASN (Agenţia Siguranţei Naţionale), ştiau multe despre internet, mult mai multe decât FBI, dar CIA nu poate, prin lege, să opereze în Statele Unite. Şi treaba ASN e să creeze (să cripteze) şi să spargă (să decripteze) coduri secrete. Totuşi, CIA a fost mereu în avangarda IT şi tehnologiei internetului.

Deşi mulţi oameni se gândesc la CIA ca la un grup de agenţi secreţi, adevărul e că majoritatea oamenilor din CIA sunt tocilari de un fel sau altul. CIA angajează de mult timp hackeri white hat şi intervievează hackeri black hat care sunt dispuşi să renunţe la viaţa de infractori (şi fac testul cu detectorul de minciuni ca să demonstreze asta). CIA are mulţi oameni care studiază sistemele bancare străine, de aici abilitatea agenţiei de a „sparge banca". Această informaţie a apărut prima dată în anii '90, când s-a aflat că CIA putea (sau deja se întâmplase) să spargă conturile bancare din străinătate ale lui Saddam Hussein sau pe cele ale teroristului Slobodan Milosević on pe cele ale lui Osama bin Laden. Această abilitate a continuat a fi neobservată (deşi a fost denunţată). Totuşi, vorbim despre străini care deţin mulţi bani obţinuţi ilegal. Pe de altă parte, băncile care sunt atacate de cyber-soldaţii CIA ezită să facă plângeri, deşi sunt proteste pe căile diplomatice. Desigur, dacă ai abilităţi de hacker ca să pătrunzi în băncile străine (care nu sunt la fel de protejate împotriva acestui lucru ca băncile din Statele Unite), ai oameni care ştiu câte ceva despre infracţiunile informatice pe internet.

Din fericire, CIA ŞI FBI, agenţii care nu s-au înţeles bine zeci de ani, au început să lucreze împreună în timpul anilor '90. Acest aspect era important pentru FBI în zona cyber-războiului, pentru că CIA are mult mai multe resurse în această zonă de care FBI are mare nevoie. Din păcate, niciodată nu sunt oameni de ajuns care să se priceapă la tehnică. FBI este încă o organizaţie care se bazează pe oameni (nu pe tehnică) şi tocilari care caută

„Angajamente" la guvern e mai probabil să prefere un CIA prietenos cu ei (care are multe locuri de muncă tehnice). De asemenea, serviciile armatei au unele locuri primitoare pentru experţii pe internet, însă doar câteva dintre ele sunt pentru civili. Deci dacă vrei să fii un cyber-războinic pentru guvern fără să mergi la taberele de recruţi, CIA a fost, şi este, locul unde trebuie să mergi.

Între timp, anul DDOS e încă prezent. Mulţi tocilari din guvern suferă de paranoia instituţională şi se aşteaptă la un nou val de atacuri DDOS. Totuşi, aceasta e una dintre problemele celor care lucrează în guvern. Pierzi contactul cu realitatea. Marile site-uri comerciale au trecut, sau tind să treacă, peste problema DDOS. Desigur, ameninţarea DDOS e încă prezentă. Dar dacă hackerii black hat vor să lanseze un atac DDOS asupra cuiva, îşi pierd timpul în încercarea de a-l folosi pe (acum) bine protejatele site-uri comerciale. Doar dacă nu vin cu o versiune nouă şi surprinzătoare de atac DDOS. E posibil, deşi apărarea lucrează neîncetat la contramăsuri pentru tipurile de atac DDOS încă nefolosite. Singura teamă reală legată de DDOS e folosirea unei noi versiuni mai periculoasă ca armă în cyber-război.

Orice tehnică DDOS veche e încă un instrument bun pentru torturarea cuiva care deţine un site cu buget mic şi aici se regăsesc cele mai multe atacuri DDOS în aceste zile. Ca să parafrazez o zicală mai veche: „bogaţii sunt mai protejaţi de DDOS, în timp ce săracii captează mai mult atenţia hackerilor black hat”.

FEDERALII PREIAU CAZUL

Din moment ce internetul e o reţea naţională, orice infracţiune comisă este o abatere federală, statală sau locală. Aceasta înseamnă că FBI trebuie să se ocupe de ea. Însă FBI dintotdeauna nu a preluat imediat noile forme de infracţiune interstatală. Dar, ca toţi cei asociaţi cu internetul, chiar şi FBI în final a trebuit să acorde atenţie. Până la sfârşitul anilor ’90, agenţii federali (FBI, Serviciul Secret, CIA, Brigada Antidrog, ATF) se dădeau peste cap să ajungă din urma valul de infracţiuni ce creştea pe internet. Desigur, FBI nu se aştepta să urmărească toţi infractorii de pe internet. Pur şi simplu, erau prea mulţi. Dar FBI a făcut ceea ce era obişnuit să facă – a urmărit cazurile de interes major. Un foarte bun exemplu de un

astfel de caz a implicat un miliardar american, hackeri ruşi, o mare companie americană, şantaj şi o maşinaţie internaţională. Într-un cuvânt, tot ce-i place FBI-ului la un caz. Mai jos este comunicatul guvernului dat la prinderea vinovaţilor. Fiţi atenţi că, de la începutul lui 2002, cei doi hackeri ruşi au încercat, fără prea mult succes, să evite extrădarea în Statele Unite. Domnul Bloomberg (acum primarul miliardar al oraşului New York) şi compania sa sunt pregătiţi să ajute la condamnarea celor doi ruşi, care probabil se vor întoarce în Statele Unite până la sfârşitul lui 2002.

14 August 2000, procurorul Statelor Unite Districtul de Sud al statului New York

MARY JO WHITE, procurorul Statelor Unite pentru Districtul de Sud al New York-ului, şi BARRY W. MAWN, împreună cu adjunctul directorului aflat la conducerea sucursalei din New York a Biroului Federal de Investigaţie, anunţă că OLEG ZEZOV, *aka* „Oleg Zezev”, *aka* „Oleg Dzezev”, *aka* „Alex”, şi IGOR YARIMAKA, cetăţeni ai Kazahstanului, au fost arestaţi pe 10 august 2000 în Londra, Anglia, pentru că ar fi intrat în sistemul informatic al Bloomberg L.P. („Bloomberg”) din Manhattan în încercarea de a sustrage bani din conturile companiei.

ZEZOV ŞI YARIMAKA sunt urmăriţi pe baza a trei capete de acuzare dezvăluite astăzi. Fiecare e acuzat de amestec în comerţ folosind şantajul, şantajarea unei corporaţii folosind mijloace de comunicare ameninţătoare şi acces neautorizat în sistemul informatic.

Conform acuzaţiilor, *ZEZOV* a obţinut acces neautorizat în sistemul informatic intern Bloomberg de la computere aflate în Almaty, Kazahstan. În primăvara anului 1999, sau cam în acea perioadă, Bloomberg furniza servicii cu date de bază prin intermediul unui program numit „Open Bloomberg” corporaţiei Kazkommerts Securities („Kazkommerts”), aflată în Almaty, Kazahstan. ZEZOV e angajat al Kazkommerts şi e una dintre cele

patru persoane de la Kazkommerts asociate contractului dintre Kazkommerts şi Bloomberg.

Mai mult, potrivit acuzaţiilor, ZEZOV a trimis un număr de e-mailuri lui Michael Bloomberg, fondatorul şi deţinătorul companiei Bloomberg, folosind numele „Alex”, cerând ca Bloomberg să-i plătească 200.000 de dolari în schimbul unor informaţii referitoare la modul în care ZEZOV a reuşit să se infiltreze în sistemul informatic.

Aşa cum se arată în acuzaţii, Michael Bloomberg i-a trimis un e-mail lui *ZEZOV* propunându-i să se întâlnească. Se crede că *ZEZOV* i-a cerut lui Michael Bloomberg să depună 200.000 de dolari într-un cont din străinătate. Bloomberg a deschis un cont la Deutsche Bank în Londra şi a depus 200.000 de dolari în cont. Potrivit acuzaţiei, Michael Bloomberg i-a propus să rezolve problema în Londra şi *ZEZOV* a fost de acord.

Cum s-a formulat în acuzaţia împotriva lui YARIMAKA, la 6 august 2000, YARIMAKA ŞI ZEZOV au zburat din Kazahstan la Londra. La 10 august 2000, YARIMAKA ŞI ZEZOV sau întâlnit cu oficialii de la Bloomberg L.P., inclusiv cu Michael Bloomberg şi cu doi ofiţeri de poliţie din Londra, unul dându-se drept director al Bloomberg L.P., iar celălalt ca traducător. La întâlnire, se pare că YARIMAKA a pretins că e un fost procuror din Kazahstan şi le-a explicat că-l reprezintă pe „Alex” şi că se va ocupa de termenii de plată. Potrivit acuzaţiei, YARIMAKA ŞI ZEZOV şi-au repetat cererile la întâlnire. La puţin timp după întâlnire, YARIMAKA ŞI ZEZOV au fost arestaţi.

Pe 11 august 2000, YARIMAKA ŞI ZEZOV au fost prezentaţi în faţa magistraturii din Londra şi le-a fost refuzată cauţiunea. Statele Unite vor cere extrădarea.

Dacă vor fi condamnaţi, YARIMAKA ŞI ZEZOV riscă până la 20 de ani de închisoare pentru amestec în comerţ folosind şantajul, doi ani pentru şantajarea unei corporaţii folosind mijloace de comunicare ameninţătoare şi un an

pentru acces neautorizat în sistemul informatic. Fiecare inculpat riscă o amendă de 250.000 de dolari, dublu faţă de câştigul brut venit de pe urma infracţiunii, sau dublu faţă de pierderea financiară a altor persoane decât acuzatul venit de pe urma infracţiunii, pentru fiecare cap de acuzare.

Domnişoara WHITE a lăudat efortul anchetatorilor Biroului Federal de Investigaţii, anchetatorilor de la Scotland Yard şi autorităţilor din Kazahstan. Domnişoara WHITE şi-a exprimat aprecierea pentru Michael Bloomberg şi Bloomberg L.P. pentru cooperare. Investigaţia e în curs.

Domnişoara WHITE a afirmat: „Internetul nu e un adăpost sigur pentru infractori. Cum demonstrează acest caz, prin cooperarea oficialilor poliţiei străine şi a companiilor americane, hackerii care folosesc internetul pentru a şantaja companiile americane şi accesează sistemele informatice cu uz intern vor fi prinşi şi trataţi cu rigurozitate indiferent de locul în care trăiesc”.

Domnul MAWN a afirmat: „Investigaţia şi acuzările ar trebui să îndepărteze ideea că, folosirea unui computer pentru comiterea unor infracţiuni la celălalt capăt al globului asigură o zonă de securitate faţă de privirea atentă a forţei poliţiei. De fapt, creşterea infracţionalităţii pe computer în ultimii ani a avut drept urmare o cooperare mai strânsă între agenţiile poliţieneşti din lume. Această investigaţie arată cooperarea dintre companiile americane şi partenerii noştri internaţionali de combatere a crimei în secolul XXI”.

OLEG ZEZOV, 27 de ani, şi IGOR YARIMAKA, 37 de ani, locuiesc în Almaty, Kazahstan. Procurorii generali ai Statelor Unite PAUL B. RADVANY ŞI JOSEPH V. De MARCO se ocupă de acuzare. Învinuirile nu sunt simple acuzaţii, iar inculpaţii beneficiază de prezumţia de nevinovăţie până la demonstrarea contrariului.

Pe lângă cazurile izolate, FBI-ului îi place să

urmărească un mare număr de cazuri ce pot fi închise şi duse 3 a judecată. Îi plac şantajul şi conspiraţiile. Ocupă prima pagină în presă şi, dacă acuzarea are succes, mulţi răufăcători ajung în închisoare.

În mai 2001, FBI a anunţat încheierea cu succes a „Operaţiunii Cyber Loss”. În urma investigaţiei au fost capturate 90 de persoane şi companii care au fraudat peste 56.000 de oameni prin intermediul internetului şi i-au înşelat pe aceşti oameni cu peste 117 milioane de dolari. Ca majoritatea operaţiunilor de acest fel, nu doar FBI a fost implicat. Centrul Naţional de Combatere a Crimei şi Centrul de Fraudă pe Internet, nou fondat de FBI la începutul anului 2000, au luat parte.

„Operaţiunea Cyber Loss” a fost o încercare a poliţiei de a băga frica în miile de cyber-infractori care operau pe internet. Centrul de Fraudă pe Internet se voia a fi un loc centralizat unde victimele infracţiunilor pe internet îşi pot denunţa pierderile. Asta însemna să dea voie tuturor celor care foloseau internetul să participe în programul „supravegherii cyber-comunităţii”. Adunând toate aceste plângeri, FBI putea cu uşurinţă să identifice cine erau marii escroci. Ca în orice alt domeniu al infracţiunilor, un mic număr de infractori dă socoteală pentru o sumă disproporţionată de fapte ilegale. Acest program operaţional dă voie FBI-ului să identifice şi să urmărească infractorii mari şi să împiedice un număr foarte mare de oameni de a mai fi înşelaţi pe viitor. A fost o operaţiune amplă.

Faza finală naţională a operaţiunii, care a adunat vinovaţii, a implicat 27 de agenţii locale ale FBI (Boston, Charlotte, Chicago, Cleveland, Dallas, Denver, Detroit, El Paso, Houston, Las Vegas, Little Rock, Miami, Minneapolis, Mobile, Norfolk, New Haven, Newark, New York, Pittsburgh, Phoenix, Portland, Sacramento, St. Louis, San Diego, San Francisco, Seattle şi Washington).

Au fost 61 de cazuri separate, ce implicau o pierdere

oficială de 117.577.000 de dolari. Însă pierderile erau mult mai mari, pentru că nu au putut fi găsite toate victimele. Dar s-a estimat un număr de 56.170 de victime. În faza finală a investigaţiei, erau 27 de operaţiuni de căutare şi arestare care au dus la 57 de arestări, înţelegeri cu procurorul sau condamnări şi 90 de puneri sub acuzare. Aceste puneri sub acuzare cuprindeau persoane cu 110 capete de acuzare, printre care fraudă pe mail, fraudă informatică, tentative la infracţiunea de furt, spălare de bani, fraudă bancară, fraudă prin telemarketing, drepturi de proprietate intelectuală (piratarea de software) şi transferul interstatal de proprietate furată.

Pentru că aceste cazuri acopereau o sferă atât de mare de infracţiuni, au fost implicate multe organizaţii de combatere a crimei. Printre acestea erau Serviciul Poştal al Statelor Unite, Fiscul (Divizia de Anchetă Infracţională), Comisia de Valori Mobiliare şi Burse, Serviciul Secret al Statelor Unite, Serviciul Vamal al Statelor Unite şi numeroase organizaţii de combatere a infracţionalităţii statale şi locale, printre care Departamentul de Poliţie din New York, Poliţia Statală New Jersey, Departamentul de Poliţie din Salt Lake City, Departamentul de Poliţie din Springville, echipa de informaticieni din Oregon, Procuratura Collège Station din statul Oregon, Departamentul de Poliţie din Texas, Departamentul de Poliţie din Seattle, Departamentul de Poliţie Monroe din statul Washington, Departamentul de Poliţie Boca Raton din statul Florida, Biroul de Control Informatic al statului Florida, Poliţia Statală Connecticut, Departamentul de Poliţie Chula Vârsta din statul California, Departamentul de Poliţie El Paso din statul Texas şi Departamentul de Poliţie din San

Diego. Un aspect tulburător al acestui caz e că, în primul an al operaţiunii, Centrul de Fraudă pe Internet a primit 36.410 plângeri şi 82% dintre ele s-au dovedit a fi valide. Acum, mulţi dintre oamenii care ajung victime pe

internet nici nu ştiu unde să facă plângeri. Interesant e faptul că victimele fraudelor pe internet tind să fie aceiaşi oameni care au căzut pradă escrocheriilor din afara internetului. Cei cu vârsta cuprinsă între 18 şi 34 de ani alcătuiesc cel mai mare grup online (cam 39% din comunitatea de pe internet). Dar şi grupul de 50 de ani şi peste e în creştere. Mai mult, utilizatorii de peste 50 de ani, probabil pentru că majoritatea sunt ieşiţi la pensie, petrec cu 19% mai mult timp pe internet decât ceilalţi utilizatori.

Utilizatorii vârstnici au mai multe avantaje decât cei tineri. Asta înseamnă mai mulţi bani pentru investiţii sau orice altă escrocherie tentanta de pe internet. Se pare că aceiaşi oameni care îi escrocau prin telemarketing pe americanii vârstnici, nu o fac pe acelaşi grup de vârstă şi pe internet.

În timp ce multe din escrocheriile de pe internet sunt făcute de aceiaşi oameni care încercau să fure bani înainte de era internetului, cea mai obişnuită infracţiune pe internet e unică în acest loc. Şi anume, nu se plătesc bunurile cumpărate la licitaţiile online. În jur de 22% din plângerile primite de FBI erau de acest fel. Sumele nu sunt mari, dar avem o mulţime furioasă de oameni. Pe locurile al doilea şi al treilea stă frauda cardurilor de credit şi a investiţiilor (fiecare cu aproximativ 5% din totalul plângerilor). Până spre finalul anilor ’90, grupurile de crimă organizată americane au început să fure pe internet. Bandele de infractori de peste ocean (mai ales în Europa de Est) au avut un avans de câţiva ani faţă de cele americane.

De fapt, FTC (Comisia Federală pentru Comerţ) s-a ocupat de problema plângerilor consumatorilor de pe internet cu câţiva ani înaintea FBI. FTC e o agenţie care se ocupă de problemele consumatorilor, nu o operaţiune poliţienească ca FBI. Dar FTC a fost primul care a observat creşterea infracţională pe internet. Multe din escrocheriile

de pe internet se bazează pe viteză. Să obţină informaţia şi s-o folosească rapid. Câteodată, nici infractorii nu înţeleg asta. Mulţi hoţi de carduri de credit sau de identitate sunt prinşi pentru că nu acţionează în timp util. În timp ce cheltuiesc bucuroşi din contul altcuiva, uită că infracţiunea nu poate fi depistată dacă schimbă cumpărăturile cu bani gheaţă şi dispar. Cumpărăturile cu cardul de credit lasă o urmă şi până şi poliţiştii ştiu că nu trebuie să blocheze cardurile (ceea ce le dă un semnal de alarmă hoţilor şi pleacă din oraş) până când pot descinde în camera de hotel în care locuiesc hoţii şi fac arestări.

FBI, FTC-ul şi alte agenţii guvernamentale dezvoltă noi tehnici de identificare, localizare şi arestare a infractorilor de pe internet în cel mai scurt timp posibil. Prin acestea nu doar că-i prind pe cei mai mulţi dintre ei, dar descurajează amatorii care deseori se gândesc (spre regretul lor) că prin infracţiunile de pe internet se fac bani uşor. E un aspect important pentru că internetul s-a dovedit a fi extrem de popular în rândul hoţilor. Priviţi cifrele. În 1997, FTC-ul primea doar în jur de o mie de plângeri de infracţiuni săvârşite pe internet. Dar până în 2000, numărul plângerilor a crescut la peste 25.000. Ce e mai rău, acesta era doar un sfert din totalul plângerilor primite de FTC şi, la acea dată, internetul acoperea doar câteva procente din comerţul din întreaga ţară.

În 2001 şi 2002, cei mai rapizi şi mai deştepţi cyber-poliţişti au efectuat sute de arestări şi puneri sub acuzare şi au speriat un număr din ce în ce mai mare de infractori amatori de pe internet. Dar perspectivele sunt încă sumbre căci tot mai mulţi hoţi profesionişti descoperă internetul. Infracţionalitatea pe internet era o afacere de 1, 6 miliarde de dolari în 2000 şi se aştepta să ajungă la 15 miliarde de dolari în 2005.

Ca rezultat al măsurilor împotriva simplelor escrocherii pe internet, cyber-infractorii sunt acum foarte probabil profesionişti. Ce e mai rău e că deseori sunt

profesionişti ce operează peste oceane. Acest lucru înseamnă implicarea mai mare a Departamentului de Stat şi a Departamentului de Justiţie. Totuşi, multe naţiuni nici măcar nu au legi împotriva multora din infracţiunile de pe internet. Şi e şi mai rău. Hoţii străini, care nu vorbesc engleza bine (necesară pentru multe escrocherii) sau cu un cazier care le-ar fi interzis accesul în SUA legal, nu mai trebuie să-şi facă griji pentru asta. Pot opera de oriunde din lume, atât timp cât au o conexiune la internet. Singurul lucru care împiedică toate acestea să producă un val uriaş de cyber-infracţiuni sunt companiile americane de carduri de credit care au înghiţit multe asemenea pierderi. Companiile de carduri de credit, care au propriile resurse considerabile antifraudă, au analizat tranzacţiile cu carduri de credit pentru semne de fraudă şi au blocat folosirea multor carduri de credit americane în afara ţării. Desigur, încă poţi merge la un dealer de maşini din Manila să-ţi cumperi o maşină nouă, dar să te aştepţi să răspunzi la întrebările cuiva la telefon (de la compania de carduri de credit) mai întâi. Majoritatea cardurilor de credit nu mai pot fi folosite pentru jocurile de noroc de pe internet şi alte operaţiuni online care dau semne de fraudă. De asemenea, băncile acordă o atenţie sporită transferurilor online de bani, un alt mod preferat de hoţi pentru a lua bani de la victime.

În ultimii 150 de ani, fiecare formă noua de comunicaţie electronică (telegraful, telefonul, internetul) a fost rapid adoptată de infractori pentru a face escrocherii. Când a apărut internetul, frauda prin telefon încă era o ameninţare ce creştea. Nu mai e cazul, având în vedere că potenţialele victime şi infractorii inventivi au trecut la mediul online. Vor mai trece câţiva ani până ce utilizatorii de internet să fie mai deştepţi şi mai atenţi la activitatea infracţională până la nivelul „normal”. Dar astea vor fi doar escrocheriile tradiţionale. Daunele ce implică software-ul şi hardware-ul de pe internet nu vor fi cu

uşurinţă domolite. Dar acesta e un cu totul alt război.

VULNERABILITĂŢI ÎN CREŞTERE

Cu numărul de utilizatori de internet în creştere, odată cu cel al oamenilor ce testează reţeaua de vulnerabilităţi, oportunităţile de săvârşire a daunelor au crescut enorm. Asta s-a întâmplat pentru că programele-cheie de software disponibile pentru hacking nu s-au dezvoltat aşa mult. De fapt, diferitele tipuri de software de internet disponibile pentru hacking au scăzut considerabil pe măsură ce competiţia a înlăturat mulţi competitori în timpul anilor ’90. Aşa se explică de ce software-ul de internet e luat la puricat de hackeri ca să găsească defecte. Găseşte un defect şi poţi face o mulţime de bani exploatându-l. Totul se rezumă la asta: nu sunt multe programe de software pe piaţă la ora actuală. Software-ul pentru servere se află pe milioane de computere şi stă la baza paginilor web, dar doar două programe diferite susţin aproape 90% din serverele de pe internet. Apache deţine 56% din piaţă şi Microsoft IIS 30%. Apoi mai sunt şi sistemele de operare şi browserele care sunt folosite pentru accesarea serverelor. Sistemele de operare Microsoft sunt pe 90% din computere şi browserul de internet al Microsoft, Internet Explorer, controlează 80% din piaţa.

Când ai câteva milioane de profesionişti de software care lucrează cu un număr redus de programe, nu se poate să nu fie descoperite defecte. De asemenea e posibil ca sutele de milioane de utilizatori să descopere defecte în programele software, dar de obicei nu ştiu peste ce au dat exact, iar din cauza naturii internetului, informaţia circulă repede. Oamenii vorbesc. De la începutul internetului, s-au obişnuit să se ajute între ei. Pentru cyber-infractori, acesta s-a dovedit a fi paradisul. Atâtea discuţii libere, uneori detaliate, despre defectele software-ului pe internet, gata de a fi exploatate. În timpul anilor ’80, hackerii exploatau

defectele cunoscute din server şi din sistemele de operare. Programele periculoase, care se foloseau de defecte, erau scrise ca exerciţii nevinovate ca să se vadă ce se putea face. Acestea erau „hack-uri” clasice. Apoi, Morris Worm a ieşit în 1988 şi a făcut mult rău. Acel „atac” a fost de fapt un accident. Până în anii ’90, hackerii black hat, care exploatau defectele de software doar de-ai naibii sau pentru a fura, s-au înmulţit. Spargerile lor intenţionate nu erau accidente.

Nu e ca şi cum ar fi mult mai mulţi programatori care o căutau cu lumânarea, dar erau şi mai mulţi cei care doreau să lucreze hackerii black hat. Deşi oamenii aleg tot mai puţine programe, serverul de internet şi software-ul browserului sunt mai mari şi mai complexe. Dacă faci ceva mai mare şi mai complex, în mod automat ai mai multe lucruri care pot merge prost. Iată, o combinaţie păcătoasă a mai multor oameni ce verifică atent mai puţine elemente ale mai multor programe de software, ce continuă să conţină mai multe defecte la fiecare actualizare.

Dintr-un anumit unghi, toate astea sunt spre bine. Marea majoritate a profesioniştilor în software îşi bagă nasul peste tot în server, în sistemul de operare şi software-ul browserului şi încearcă doar să facă programele să lucreze sigur şi eficient. Când găsesc un defect, îl raportează. Şi prin multele raporturi ale erorilor, producătorul de software va repara acel lucru imediat. Ei bine, nu întotdeauna. Producătorii de software fac bani creând noi programe de software, nu reparându-le pe cele vechi. Microsoft, în special, e vulnerabil aici. Microsoft nu doar produce noi programe de software, dar vine cu noi versiuni ale produselor existente aşa frecvent că unele sunt versiuni ale vechilor programe aflate încă în uz. E mai puţin probabil ca vechile versiuni să fie reparate. În mod ironic, cele mai bine menţinute (fără erori şi reparate rapid) două părţi ale software-ului de internet (software-ul pentru serverul Apache şi sistemul de operare Linux) sunt

software-urile de tip *open Source.* De fapt, nimeni nu le deţine, ci o reţea de utilizatori şi voluntari le menţin. Suna ciudat, dar funcţionează. Linux nu e o ameninţare pentru Microsoft în domeniul sistemelor de operare, dar Apache deţine de fapt majoritatea pieţei.

Software-ul Microsoft nu e *open Source* şi celor de acolo nu le place să repare toate erorile (e scump). Cu cât e mai mare perioada dintre descoperirea noilor erori şi repararea acestora, cu atât e mai mare oportunitatea infractorilor să îşi dea seama cum să exploateze eroarea şi să lanseze programe periculoase pe internet ca să se folosească de eroare. Aceste probleme sunt cauza a mai mult de jumătate din atacurile hackerilor despre care auziţi.

Soluţia Microsoft la problemă e să militeze pentru o lege care să facă ilegala raportarea unei erori altcuiva în afară de guvern şi de producător. Posteaz-o la vedere şi te-ai ars: ai FBI-ul la uşă şi urmează punerea sub acuzaţie. Logica celor de la Microsoft e că, atunci când aceste erori sunt anunţate public, băieţii răi au timp să pună la cale un mod prin care să exploateze problema. Are sens, dar de obicei cele mai rele defecte sunt descoperite de oameni diferiţi sau de un grup de oameni în acelaşi timp. Asta-i îngrijorează pe cei mai mulţi utilizatori pentru că au impresia că, fără presiunea generată de publicitatea pe care o au erorile lor, Microsoft le va rezolva cu greu. Oamenii văd în acest aspect mai mult decât văd cei de la Microsoft dezavantajul anunţurilor publice.

Fără îndoială, sunt multe erori. În 2000, au fost găsite 1.090 de erori în software-ul de internet, dintre care 4% puteau fi folosite de hackeri pentru a provoca daune serioase. În 2001, au fost găsite 2.437 de erori, dintre care 13% puteau fi exploatate de hackeri. Se poate spune că era cyber-războiului a fost creată de programele de software cu erori în creştere şi de hackerii răi.

Guvernului Statelor Unite nu-i place această situaţie.

La începutul anului 2002, forţele aeriene ale Statelor Unite, care de obicei iau iniţiativa în problemele cyber-războiului, au avertizat firma Microsoft să îmbunătăţească protecţia software-ului lor repede sau vor risca să-şi piardă cel mai mare client al lor, guvernul Statelor Unite. Vânzările software-ului Microsoft către guvernul Statelor Unite (direct sau indirect prin software-ul instalat în hardware) se ridică ia miliarde de dolari pe an. Guvernul cumpără de mult timp software-ul Microsoft pentru că e cel mai ieftin şi uşor de instalat (dacă nu chiar cel mai uşor de folosit). Dar cum tot mai mulţi oameni au locuri de muncă dependente de internet, protecţia şi siguranţa software-ului Microsoft a devenit o problemă. Şi ameninţarea nu e una fără temei. Sunt tot mai multe voci în interiorul forţelor aeriene care ar prefera un sistem de operare Linux mai ieftin şi mai sigur. În timp ce Linux nu poate derula multe din jocurile populare pe computerele ce folosesc sistemele de operare Microsoft, forţele aeriene vad acest lucru ca pe un plus. Şi majoritatea software-urilor de care au nevoie forţele aeriene sunt disponibile pe computerele ce folosesc Linux. Dar este şi un mare dezavantaj. China a adoptat Linux-ul ca sistem de operare standard (pentru guvern şi şcoli). Asta înseamnă că programatorii chinezi vor fi mai familiarizaţi cu Linux decât cu Microsoft şi astfel mai capabili să spargă sistemele Linux.

Numărul de erori grave găsite în software-ul Microsoft e uluitor. La sfârşitul anului 2001, numărul de erori de protecţie cunoscute erau:

Software folosit pentru funcţionarea internetului, sau conectarea la internet, şi un număr mare de defecte pentru fiecare.

Microsoft Outlook şi Outlook Express: 20 (deşi acestea sunt două programe separate, unele defecte se puteau găsi la ambele).

Microsoft Internet Information Server: 44 (nu doar că

erau mai multe defecte decât în Apache, dar problemele erau şi mai serioase).

Microsoft Internet Explorer: 47 (cel mai folosit browser web şi cel mai periculos de folosit).

Microsoft Windows 2000: 79 (sunt descoperite cam trei noi vulnerabilităţi pe lună de la lansarea sa).

Microsoft Windows 98: 25 (acum e un sistem de operare mai vechi şi încă periculos de folosit).

Apache: 29 (cel mai folosit şi cel mai sigur software de server web).

Debian Linux: 28.

Sistemul de operare MacIntosh: 2 (versiunea mai veche de software MacIntosh şi cel mai sigur sistem de operare existent).

Sistemul de operare Mac X: 10 (cel mai nou sistem de operare lansat de MacIntosh). În acel timp, noul sistem Windows XP scos pe piaţă, proclamat ca cel mai sigur sistem de operare Microsoft din toate timpurile, s-a dovedit a fi în schimb la fel de plin de erori ca Windows 2000. Mai mult, existau sistemele răspândite (pentru afaceri) de software de baze de date online (ca Oracle). Acest software era montat diferit pentru fiecare site, dar cam 12% din toate bazele de date online erau sparte în 2001.

Din câte se ştie, nu sunt totuşi atât de mulţi hackeri răi (black hat) care să exploateze vulnerabilităţile acestor programe de software. Hackerii white hat şi administratorii de reţea sunt mai liniştiţi din cauza lipsei de exploatare. Dar în acelaşi timp, **hackerii** white hat în special sunt conştienţi de gradul de daune ce pot fi făcute. Un mod de a privi lucrurile e că cei mai buni din hackerii black hat ar folosi mai degrabă aceste defecte de protecţie ca să facă bani. Asta înseamnă că defectele sunt exploatate ca să fure informaţii sau bani. Cauzarea multor daune doar atrage atenţia de la lege şi un hacker black hat priceput nu

vrea să atragă atenţia. Dar în acelaşi timp, e foarte probabil ca cyber-luptătorii militari să cerceteze atent aceste defecte pentru a le folosi în situaţiile din timpul războiului. Aşa că nu te culca pe-o ureche pentru că un mare număr de vulnerabilităţi nu sunt exploatate imediat ca să ne dea dureri de cap.

De asemenea, gândeşte-te că majoritatea atacurilor raportate pe internet în 2001 au fost cauzate de doar trei viruşi. Şi e foarte probabil ca aceşti trei viruşi să fie eliberaţi de trei persoane. Sunt multe daune (miliarde de dolari să facă curat) provocate de trei e-mailuri. Au mai fost mii de atacuri individuale asupra computerelor neprotejate şi ser-verelor pentru a instala programe zombie pentru atacuri DDOS sau mai multe alte comportamente antisociale similare. Cele mai serioase atacuri, împotriva site-urilor comerciale, în scopul furtului, probabil au fost cu sutele. Multe din „atacuri”, într-adevăr majoritatea, erau automate.

Doar că nu sunt mulţi oameni pricepuţi care să intre pe un site protejat şi să rişte să fie prinşi doar pentru a se distra sau să facă bani.

Majoritatea escrocheriilor de pe internet nu implicau vrăjitori programatori care să repare software-ul cu probleme, ci simpli infractori de modă veche ce lucrau într-un domeniu nou. Cu un număr crescut de defecte ce apăreau în software-ul de internet, creşteau riscurile pentru noi toţi.

Din fericire, oamenii care aveau cel mai mult de pierdut, mai ales site-urile comerciale, sunt la fel de prompţi în apărarea site-urilor lor precum hackerii black hat în atacarea acestora. Majoritatea computerelor cu defecte (Microsoft) serioase sunt folosite de oamenii obişnuiţi. Combinaţia dintre computerele puternice din mâinile milioanelor de utilizatori, cu răspândirea conexiunilor rapide le dau hackerilor black hat şi cyber-războinicilor un nou câmp de luptă gata de a fi folosit.

Dacă un cyber-război izbucneşte şi nu ai un asemenea computer, aşteaptă-te să faci parte din „victimele colaterale”.

AUTOSTRADA PĂRŢII ÎNTUNECATE

Atacurile militare, precum apa, urmează calea ce nu opune rezistenţă. Un asemenea exemplu e una din cele mai evidente forme de cyber-război pe internet, atacul DDOS. Apărut pentru prima dată în 1999, până la sfârşitul lui 2001 erau peste 500 de atacuri DDOS pe zi asupra site-urilor web şi aparatelor conectate la reţea (de exemplu imprimantele). DDOS a devenit o jucărie favorită pentru mulţi script kiddies, căci le permite să se furişeze în computere neprotejate, să lase programele zombie de care au nevoie să lanseze atacul DDOS, apoi să aleagă un site web care nu le place şi să-şi activeze programele ca să lanseze atacul DDOS şi, apoi, să blocheze site-ul. De asemenea, programele zombie pot fi folosite a se infiltra în site-ul pe care sunt instalate. Site-urile comerciale şi companiile producătoare de software antivirus s-au concentrat rapid asupra problemei. Dar acest lucru funcţiona doar pentru oamenii care erau conştienţi că au o problemă, ştiau că se putea repara, aveau timp şi erau interesaţi să-şi protejeze serverele de programele zombie. Dar aşa cum atacurile DDOS lansate de zombie apăreau în peisaj, la fel apăreau şi milioane de utilizatori de computer cu modemuri pe cablu şi conexiuni DSL. Acestea erau locurile perfecte în care programele zombie se puteau ascunde. În timp ce script kiddies ţineau socoteala programelor zombie pe care le puteau planta şi cât de greu se putea pătrunde pe un site, computerele individuale cu conexiuni „mereu deschise” şi rapide erau şi mai bune. Site-urile comerciale şi cele ale universităţilor erau destul de bine protejate. Pe cât era de sigur să lansezi un atac DDOS, pe atât de periculos devenea să plantezi programele zombie. Site-urile comerciale erau din ce în ce

mai echipate cu detectoare de acces neautorizat şi oameni gata pregătiţi care puteau depista intrusul. Federalii te puneau imediat sub acuzare. Treaba asta, zombie şi DDOS, nu era distractivă dacă erai prins.

Dar utilizatorii cu modemuri pe cablu cel mai probabil habar nu aveau de ceea ce se întâmpla în interiorul computerului lor. Aceştia nu se prindeau şi probabil nici nu observau programul zombie la treabă până ce nu ajungeau acasă şi descopereau că nu mai au conexiune la internet şi găseau un mesaj pe telefon de la compania de cablu pentru a apela la suportul tehnic să-şi „deviruseze calculatorul”. Chiar dacă mulţi utilizatori de modemuri pe cablu aveau un firewall şi software antivirus, pentru hackeri era mai uşor să se ocupe de asta decât de o vizită de la FBI.

Poate şi mai ameninţător, computerele personale au devenit locul principal de lansare a atacurilor în cyber-război. O naţiune inamică putea amplasa rapid programe zombie militare pe mii de computere personale, computere cu o mare capacitate de a accesa internetul. Ca să mai vorbim de „duşmanul dintre noi”. O asemenea putere putea închide site-urile militare şi guvernamentale zile întregi, sau săptămâni, cu atacuri DDOS (şi similare), chiar dacă Statele Unite îşi întrerupeau conexiunile la internet cu restul lumii. Tot ce trebuia să facă atacatorul era să programeze programele zombie militare să treacă la „Planul B” dacă nu primeau instrucţiuni de acasă într-o anumită perioadă de timp. Depistarea tuturor programelor zombie militare putea dura luni întregi, căci majoritatea erau pe computere folosite de oameni care nu aveau prea multe cunoştinţe tehnice. Din cauza protecţiei scăzute a majorităţii computerelor personale, programele zombie militare puteau lansa atacuri cu viruşi care să se instaleze la rândul lor în mai multe computere personale.

Atât timp cât unul din ele era încă activ, atacurile puteau reîncepe.

Programele militare zombie sunt o armă perfectă, necruţătoare, eficientă, se multiplică singură, e greu de detectat şi ieftină. Vulnerabilitatea la atacuri de acest gen va dispărea în curând. Într-adevăr, nu vor dispărea niciodată de tot, dar toţi se străduiau încă din 1999 să dezvolte modalităţi mai bune de protecţie. Asta e uşor de făcut, în comparaţie cu înlăturarea atacatorului. Încă puţin science fiction lua viaţă. Bun venit în secolul XXI!

AVEŢI CÂŢIVA VIRUŞI?

În 2001, Departamentul Apărării s-a arătat iritat când a aflat că marile companii americane de software ofereau Chinei copii ale viruşilor mortali care nu fuseseră „în sălbăticie”. Din peste cei 70.000 de viruşi informatici descoperiţi în ultimii 20 de ani, mulţi dintre cei letali nu au fost niciodată lansaţi în reţea (trimişi „în sălbăticie”). Unii dintre aceşti superviruşi au fost „în sălbăticie” pentru puţin timp înainte să dispară (pentru că erau programaţi să se autodistrugă, sau din cauza unui defect conceptual care îi împiedica să se răspândească). Puţinele companii care produc software antivirus menţin arhive cu cât de mulţi viruşi pot păstra. Pentru cineva care construieşte un arsenal de viruşi informatici militari, aceste arhive sunt o resursă valoroasă.

Având în vedere atitudinile afişate de guvernul chinez referitoare la cyber-război şi la Statele Unite (chinezii vor să-l folosească pe primul împotriva celuilalt), acest export a iscat tensiuni la Pentagon. Totuşi, ca orice lucru care implică China şi computerele, nu totul e ce pare a fi. China dorea copii ale acelor viruşi ca să poată testa software-ul antivirus pe care-l cumpăra. Firmele americane şi-au imaginat că acţionează din politeţe, având în vedere că erau destul de siguri că nu erau singurii care deţineau aceşti 300 de viruşi. Poate asta era tot. La urma urmei, cu un an înainte, chinezii au promulgat o lege care pedepsea sever pe or cine lansa viruşi. China a început să aibă tot

mai multe probleme cu viruşii în toată perioada anilor ’90. Hackerii chinezi lansau viruşi creaţi să facă mai mult rău computerelor aflate în China. În acelaşi timp, au existat unii viruşi nou creaţi lansaţi în 2001, care proveneau din China. Unii ar putea spune că China voia acces la acele arhive americane cu viruşi din cu totul alte motive.

La sfârşitul anului 2001, erau peste 71.000 de viruşi identificaţi „în sălbăticie” (găsiţi pe un alt computer decât cel pe care au fost creaţi). Cu zece ani înainte, existau aproximativ o mie de viruşi cunoscuţi, în decembrie doar, în 2001, 1.256 de noi viruşi au fost descoperiţi. Acum, majoritatea viruşilor existenţi sunt fie scoşi din uz (hardware-ul sau software-ul pe care au fost creaţi să-l atace nu mai există, sau sunt foarte rar conectate la internet) sau relativ inofensivi. Unii au fost creaţi să fie inofensivi, alţii nu erau creaţi cum trebuie şi nu funcţionau cum trebuie. Mai mult, mulţi din viruşii „noi” sunt doar versiuni ale celor vechi. Şi, câţiva din ei tind să provoace majoritatea daunelor. În decembrie 2001, peste 90% din atacurile cu viruşi raportate erau făcute de un singur virus, Badtrans-B (o versiune a originalului Badtrans). Acesta se răspândea ca ataşament la e-mail când era trimis sistemelor ce foloseau Microsoft Outlook.

Poţi cumpăra, sau lua gratis de pe internet, kituri „cum să „pentru crearea viruşilor. Crearea lor a devenit un hobby fascinant, unu spun că provoacă dependenţă pentru mulţi programatori şi ingineri de reţea. De obicei, se face schimb liber de idei, sau cel puţin sunt postate în locuri de unde ceilalţi le iau şi le duc mai departe. Se pare că sunt şi creatori de viruşi izolaţi, şi destul de buni, care comunică doar prin munca lor. Le e teamă că unii din ei, sau armata chineză, vor dezvolta un „doomsday virus” care va închide întreg internetul. Acest lucru e posibil teoretic, cel puţin pentru un timp, dacă ataci computerele specializate (numite rutere) care controlează munca din culise de pe internet.

Ca majoritatea terorilor necunoscute, acesta are un sâmbure de adevăr în el. Şi precum se întâmplă în cazul armelor apocaliptice, cea mai bună apărare e să ai şi tu una. Cum acest lucru a mers cu armele nucleare (cea mai mare armă „apocaliptică”), o armă pe internet de calibrul acela va merge doar dacă ceilalţi ştiu că o ai. Dar dacă le spui asta, trebuie să le-o explici ca să fie credibilă. Totuşi, dacă le dai detalii referitoare la virusul tău apocaliptic, pot fi luate contramăsuri care-l vor reduce de la statutul de „apocaliptic” ta, să spunem, „pacoste”.

Probabil China nu doreşte să creeze un virus apocaliptic, doar viruşi letali şi asta e destul de rău.

MICROSOFT PATRIOTUL

Lipsa de software de protecţie pentru computerele personale le-a înlesnit munca infractorilor de pe internet. Aceste instrumente vulnerabile erau perfecte pentru lansarea de atacuri militare de către cyber-râzboinici. Singurul mod de protecţie a serverelor comerciale şi militare e actualizarea sistemelor de operare de pe computerele personale. Nu e aşa de greu pe cât parc, căci cel mai slab punct e sistemul de operare şi lipsa firewall-ului şi a software-ului antivirus. Microsoft era binecunoscut în anii ’90 pentru software-ul slab protejat. Dar eforturile de a îmbunătăţi calitatea au eşuat lamentabil. Marea majoritate a breşelor de securitate şi a atacurilor asupra utilizatorilor de pe internet erau din cauza defectelor software-ului Microsoft. La începutul anului 2002, Microsoft a anunţat că vor face din crearea mecanismelor de protecţie principalul lor ţel. Acesta era un mesaj încurajator, căci compania a demonstrat în trecut că poate să-şi focalizeze interesul în funcţie de problemele existente.

Presiunea asupra Microsoft a fost mare, nu doar din cauza denunţurilor publice şi a comunicatelor de presă ale organizaţiilor ce anunţau renunţarea la software-ul

Microsoft. Aşa că, era o problemă comercială pentru cei de la Microsoft. Dar, de asemenea, au fost şi şedinţele informative de la Departamentul Apărării şi părerea unor oficiali guvernamentali ce se ocupă de protecţia computerelor despre faptul că starea proastă a software-ului Microsoft punea în pericol siguranţa naţională. Mai mult, Departamentul Apărării e cel care plăteşte miliarde de dolari firmei Microsoft în fiecare an. Probabil că 11 septembrie 2001 a jucat un rol în acest demers. Dacă Departamentul Apărării era şantajat, putea spune că teroriştii sunt ajutaţi în atacurile pe internet de defectele impardonabile de protecţie ale software-ului Microsoft.

Microsoft poate repara multe dintre defectele de protecţie folosind actualizările periodice pe care le scoate pe piaţă pentru software-ul său. Acestea pot include caracteristici suplimentare de firewall, antivirus şi software special creat pentru a fi folosit de utilizatorii DSL aflaţi „mereu online”. Cel mai nou sistem de operare Microsoft, Windows XP, are firewall inclus. Dar e nevoie de mult mai mult pentru a furniza o protecţie eficientă, mai ales să găseşti şi să elimini multe din defectele de protecţie înaintea lansării unui nou software. Multe se pot face într-un an sau mai mulţi dacă problema ar fi abordată direct. Şi Microsoft ştie cu ce are de-a face. Un motiv pentru multele defecte de protecţie în software-ul Microsoft e efortul de a-l face cât mai uşor utilizabil pentru oameni. Apple se află de mult timp în faţa celor de la Microsoft la capitolul „uşor de folosit” şi chiar Bill Gates a spus că un computer ideal e „unul pe care mama să-l poată folosi”. Apple are mai puţine probleme de protecţie, pe de o parte pentru că sunt mult mai multe computere ce folosesc Microsoft, pe de alta pentru că toate computerele Apple au software de reţea integrat în sistemul de operare şi acorda o mai mare importanţă protecţiei.

Dacă va fi un mare cyber-război în următorii câţiva ani, numeroasele defecte din software-ul Microsoft vor fi

scoase ţap ispăşitor ca având o contribuţie mare la indiferent ce daune vor suferi Statele Unite. Aceasta nu e genul de moştenire pe care o companie vrea s-o lase-n urma sa, mai ales că o întrevedem.

CAPITOLUL 11
CUM SĂ SUPRAVIEŢUIEŞTI CYBER-RĂZBOIULUI

Dacă nu vrei să fii o victimă a cyber-războiului, uite ce poţi face şi cum să te păzeşti. Sunt şi unele lucruri importante pe care ar trebui să le ştii despre companiile producătoare de software de internet.

MICROSOFT CEL RĂU

Corporaţia Microsoft este deseori descrisă ca fiind singura companie ce are cea mai mare responsabilitate pentru problemele de protecţie ale utilizatorilor de internet. În mare parte e adevărat, doar pentru că Microsoft e cel mai mare furnizor de software pentru utilizatorii de internet şi pentru mulţi furnizori de internet. Unele din probleme, să se noteze asta, nu puteau fi evitate. De exemplu, cine a creat sistemul de operare folosit pe majoritatea computerelor personale ar ajunge să aibă un nou produs care ar fi cercetat îndeaproape de hackeri pentru puncte slabe. Fără îndoială, ar exista puncte slabe, pentru că un sistem comercial de operare în masă ar trebui să se preocupe de cererea în continuă creştere de hardware şi software noi, compatibile. Sistemele de operare Microsoft deţin 90% din piaţa în parte pentru că au făcut un efort să susţină majoritatea software-ului şi hardware-ului vechi şi tot ce a apărut nou. Aceasta a dus la mărirea complexităţii sistemelor de operare. Multe lucruri pot merge prost într-o astfel de situaţie. Presiunea asupra distribuirii de noi versiuni ale sistemelor de operare ar însemna că repararea problemelor de compatibilitate ar fi mai importantă decât protecţia pe internet. Mai mult,

sistemele de operare Microsoft au fost create înaintea apariţiei internetului, sau a utilizării excesive pe modemurile computerelor. Aşa că, multe obiceiuri proaste, care nu erau serioase înainte de internet, au devenit fatale odată cu apariţia sa. Cel mai bun exemplu e problema „buffer overflow”. Practic, aceasta e o eroare de programare ce nu apare întotdeauna, ci doar dacă programul nu ia combinaţia corectă de instrucţiuni şi de date. Rezultatul e blocarea programului. Înainte de apariţia internetului, programatorii reparau problemele buffer overflow-ului când le descopereau şi nu testau noul software ca să le găsească. Dar când un program ce mergea pe internet (un browser sau un software de server) are probleme buffer overflow, acest defect poate fi exploatat de un hacker pentru a introduce un program pe un site web sau pe un computer. Şi noul program poate fi folosit de către programatorii rău intenţionaţi pentru a prelua controlul asupra unui server sau computer. Programatorii Microsoft care au creat software-ul de internet nu au dat prea multă atenţie problemei buffer overflow, văzând-o doar ca pe unul din multele lucruri ce pot merge prost într-un program. Programatorii care au lucrat la software-ul de comunicare de date întreaga lor carieră au dat atenţie şi au fost mult mai rapizi în stoparea problemelor buffer overflow. Acesta e un motiv pentru care programul serverului Microsoft IIS e mult mai uşor de atacat decât software-ul serverului Apache creat de Unix. Apache nu e doar de două ori mai stabil decât IIS ca operare, ci are mai puţin de o zecime din numărul de erori care ameninţă protecţia internetului.

Microsoft nu doar că a produs multe programe software de server pentru internet pline de defecte, dar a schimbat licenţele software pentru a „încuraja” clienţii să nu folosească altceva în afară de Microsoft. Asta a descurajat firmele care foloseau software-ul

Microsoft pentru uz intern de la a mai folosi

software-ul de server Apache mai sigur pentru serverul site-ului lor.

Un motiv pentru care Apache era un software mai bun, pe lângă erorile mai puţine, era felul în care serverul Apache era instalat de utilizator. Când un utilizator instala serverul Microsoft IIS, toate opţiunile erau activate. Chiar şi pe un server web, sunt multe opţiuni de care nu are nevoie nimeni. Şi unele dintre acestea, chiar dacă nu sunt folosite, sunt un alt mijloc pentru hackeri de a intra. Când instalezi Apache, aproape toate opţiunile sunt dezactivate. Dacă vrei unele extraopţiuni, trebuie doar să le activezi, dar acea procedură se asigură că ştii ce faci, sau că vrei să afli.

Dar a fost mai rău. Software-ul de server Microsoft era prea vulnerabil pentru că se adresa utilizatorului de categorie mică şi mijlocie

Acestea sunt organizaţiile cu oameni care nu observau problemele software-ului înainte să declanşeze un fel de dezastru transmis pe internet. De asemenea, aceste organizaţii cuprind cele mai mari segmente de utilizatori de internet (vorbim aici de companii diferite). Conceptul designului software-ul Microsoft era să-i facă instalarea şi utilizarea cât de simplă posibil. Astfel, cum erau multe opţiuni de care nu era nevoie, dacă erau toate activate, de obicei se loveau una de alta. Era foarte deştept, dar ignora în mare problema vulnerabilităţii la hackeri. Când a început să se arate cu degetul la Microsoft, reacţia a fost de genul „Cine? Noi?”. Programatorii de la Microsoft nu dădeau impresia că nu verificaseră protecţia pe internet sau că luaseră în serios problema.

Oricum, majoritatea utilizatorilor de internet nu vor avea mult de furcă cu software-ul de server defectuos. Nu, o să ai de suferit (dacă nu s-a întâmplat deja) dacă foloseşti programul Microsoft Outlook. Cel mai folosit program de e-mail de pe planetă, Outlook-ul este şi motivul pentru care

majoritatea oamenilor sunt atacaţi de viruşi. Problema e a „Opţionalelor”. E un obicei Microsoft acela de a adăuga tot mai multe opţiuni programelor, chiar dacă marea majoritate a utilizatorilor nu vor avea nevoie niciodată de ele. Dar pentru a justifica lansarea noilor versiuni de pagini de lucru în Excel sau a programelor de procesare a cuvintelor în Word, sunt adăugate mai multe opţiuni: au o corporaţie de condus, angajaţi şi acţionari de luat în considerare. În sine nu e o problemă majoră, opţiunile rar folosite sunt ascunse şi majoritatea utilizatorilor nu le observă.

Dar „suportul pentru scripting” era o opţiune care deschidea oportunităţile rele pentru hackeri. Scriptingul nu e nimic mai mult decât un sistem ce permite unui programator, sau utilizator, să scrie o listă de comenzi într-o pagină care să fie executate automat. Scriptingul e o opţiune veche. Fişierele *batch* (BAT) din anii ’80 erau fişiere script şi erau foarte populare în rândul utilizatorilor de atunci. Chiar şi înainte, limbajele scripturilor erau esenţiale pentru rularea uşoară a sistemelor de mare viteză de atunci. Microsoft a observat popularitatea scriptingului şi i-a extins utilizarea. Cu introducerea Visual Basic în anii ’90 şi integrarea sa în alte aplicaţii în 1993 (mai întâi Excel, apoi Word), scriptingul era disponibil în aceste programe şi mai ales, oriunde într-un computer echipat cu Windows. Când Windows 98 a fost introdus, acesta instala automat suportul pentru scripting în toate aplicaţiile Windows. Nu le lua mult programatorilor rău intenţionaţi să-şi dea seama ce oportunităţi de hacking prezenta acesta. Primii viruşi transmişi prin email ce foloseau scriptul în fişierele Word sau Excel au apărut în 1997. Acest lucru a dus la întâmplări nefericite, precum viruşii Melissa şi I Love You. De aici lucrurile au mers rău, în ciuda faptului că marea majoritate a utilizatorilor nu aveau nevoie de aşa mult „suport” pentru scripting.

Microsoft nu era de vină aici. Microsistemele Sun au

dezvoltat limbajul Javascript în 1995 pentru utilizarea pe browsere web. Chiar şi Microsoft l-a adoptat, deşi şi-a adăugat propriile idei cu scriptingul ActiveX. ActiveX permitea viruşilor să fie descărcaţi fără cunoştinţa utilizatorilor de pe site-urile web. Acest lucru dădea voie viruşilor să fie conţinuţi în mesajele ce permiteau HTML-ul (de genul paginilor web) citite pe e-mail. Primul din acestea a fost virusul Kak, care a apărut spre sfârşitul anului 1999. Dacă deschideai e-mailul şi scriptingul era activat, Kak lucra şi făcea schimbări în sistem. Mai întâi, se ataşa emailurilor trimise. O dată pe lună afişa un mesaj şi închidea Windows-ul.

Microsoft a reuşit să înrăutăţească situaţia. O altă opţiune în Outlook e posibilitatea de a amplasa un program într-un e-mail chiar dacă scriptingul nu era activat. Când Microsoft a fost alertat asupra problemei în 2001, sfatul lor era să nu începi un e-mail cu „begin” (cuvântul magic care făcea Outlook-ul să creadă că orice se întâmpla după era un ataşament codificat).

Presiunea utilizatorilor şi-a făcut efectul asupra Microsoft în 2002. Microsoft a declarat că protecţia urma să fie prioritatea numărul unu în viitor. Putea fi doar simpla recunoaştere a unei alte pieţe în creştere. În 2001, vânzările de software de protecţie au ajuns la 3, 6 miliarde de dolari şi vor ajunge la peste 5 miliarde până în 2003. Companiile care furnizează servicii de protecţie a reţelei (consultanţă, servicii online) au trecut de la 720 de milioane de dolari în 2000 la peste un miliard în 2002 şi se aşteaptă să-şi dubleze profitul până în 2005. O parte a acestui lucru e că programatorii Microsoft vor fi prea ocupaţi cu rezolvarea problemelor de securitate şi că vor avea mai puţin timp să adauge mai multe opţiuni nefolositoare. Dar mai întâi va trebui să existe o acţiune a Microsoft şi acest lucru va lua timp. Atitudinea asupra erorilor găsite în software-ul său era, în mod normal, că, dacă numărul acestor defecte putea fi ţinut sub un anumit

nivel, programatorii puteau continua să adauge opţiuni şi să scoată noi produse. Pentru Microsoft, acesta era un mod bun de a face afaceri. Industria software-ului pentru computere, de la început (la sfârşitul anilor ’70), era dominată de mulţi amatori şi antreprenori. Producătorii şi clienţii s-au obişnuit să caute ce e nou şi totodată să înveţe să trăiască cu orice eroare. Majoritatea utilizatorilor nu mai întâlniseră un computer înainte să cumpere Windows, dar să mai şi folosească unul. Toţi am învăţat să tolerăm produsele disponibile pentru că nu exista ceva mai bun. Dar astăzi, erorile software-ului de protecţie pe internet au un efect notabil asupra utilizatorilor. Întreabă pe oricine care are computer şi a avut viruşi.

E posibil să fabrici software fără erori (sau ceva apropiat de asta), în general se întâmplă acest lucru pentru aplicaţiile industriale şi militare. Auzi de ele doar atunci când erorile apar, pentru că asemenea evenimente sunt rare. Dar în general sunt fără erori. Şi japonezii produc software fără erori. Costă mai mult să-l creeze, iar munca nu e aşa „distractivă” pentru programatori. E nevoie de multă disciplină şi de un management acerb să produci software fără erori. Evident, Microsoft nu e singura sursă de software cu defecte de pe internet, dar e cea mai mare şi asta îl face cel mai expus atunci când încerci să clarifici situaţia.

Pentru a reduce numărul de erori, Microsoft ar trebui să facă schimbări serioase în modul de operare al programatorilor. Se poate face, dar nu imediat. Microsoft şi-a luat angajamentul la începutul lui 2002. Înainte de sfârşitul lui 2002, puteai vedea aplicarea acestor măsuri la unele produse Microsoft. Nu e uşor, dar e posibil, şi dacă nu se întâmplă, internetul va avea mari belele.

INTERNETUL INVIZIBIL

Când lucrurile merg prost pentru tine pe internet, sau din cauza lui, e posibil să nu fie ceva din computerul

tău care cauzează problema, sau ceva de pe site-urile pe care le vizitezi. Mai mult, problema pot fi hackerii care fac rău pe „internetul invizibil”. De ani de zile, se credea că ruterele, serverele DNS şi software-ul de bază care făceau tot ceea ce este invizibil (pentru utilizatori cel puţin) pe internet să se mişte eficient, erau sigure. Dar la începutul anului 2002 s-a descoperit că de zece ani exista un defect (cunoscut ca „vulnerabilitatea SNMP”) în software-ul ruterului care îi permitea cuiva cu îndemânarea potrivită să închidă ruterele sau să preia controlul asupra lor. Hackerii black hat discutau deseori să închidă internetul dintr-o ţară întreagă. Acestea sunt glumele pe care ei le gustă. India şi China sunt menţionate deseori.

Ambele ţări au o infrastructură relativ redusa pentru funcţionarea internetului, în plus, în aceste ţâri există şi probleme culturale (hackerii pot fi la fel de naţionalişti şi nesiguri ca orice alt grup).

Mulţi programatori americani sunt puţin ofensaţi de mulţii programatori indieni prost plătiţi (dar supercalificaţi) care le iau „locurile de muncă”. Programatorii indieni care emigrează în Statele Unite de obicei ocupă poziţii sus-puse (sau pun bazele propriei companii) prin muncă grea şi calificări superioare. Asta-i supără pe unii, aşa că ideea de a închide internetul Indiei e un vis des întâlnit.

Punctele slabe recent descoperite ale ruterelor aduc asemenea fantezii mai aproape de realitate. China nu trimite la fel de mulţi programatori în Statele Unite, dar aceştia sunt naţionalişti şi apar des altercaţii între hackerii americani şi chinezi. Închiderea internetului în China, măcar pentru câteva zile, e văzută ca cel mai nou hack „poţi face asta”. Pentru cyber-războinici, posibilitatea de a bloca sau de a prelua controlul asupra unor reţele de internet are o valoare militară reala. Înainte de începutul anului 2002, problemele SNMP erau descoperite, deja se ştia că ruterele şi serverele DNS aveau puncte slabe. Dar

problema SNMP furnizează hackerului răuvoitor o armă mai precisă. Prin exploatarea punctelor slabe ale SNMP (prin schimbarea software-ului cu care funcţionează ruterul) hackerii pot opri sau devia mari părţi ale traficului pe internet. Nu pentru mult timp, căci proprietarii acelor rutere puteau în final rezolva problema. Dar impactul unui asemenea atac atrage atenţia mass-media pe care o caută hackerii. Acesta e mai mult un risc militar decât majoritatea punctelor slabe de pe internet. Posibilitatea închiderii internetului unei naţiuni sau regiuni, pentru ore sau zile, umileşte victimele, forţele poliţieneşti şi militare. Sunt şi alte defecte cunoscute sau suspectate pe „internetul invizibil" şi acestea rămân o problemă pentru perioada următoare. E ceva pentru care să te îngrijorezi şi mulţi oameni care folosesc internetul nu dorm din cauza asta.

JOCUL DE-A APĂRAREA

Sunt multe lucruri pe care le fac profesioniştii pentru a păstra în siguranţă site-urile militare şi comerciale, ce pot fi folosite de utilizatorii cu buget restrâns.

Ce mai grea tehnică e setarea computerului, reţeaua de acasă sau de birou, astfel încât să nu mai existe probleme. Acest lucru înseamnă că vei putea fi atacat de hackeri, ce pot afecta o parte a sistemului tău, dar nu-l vor închide complet. Pentru că e greu de făcut acesta pentru un singur computer, profesioniştii se folosesc de mai multe computere dinadins îşi instalează sistemele în aşa fel încât, în eventualitatea unui atac sever, să pice doar o parte din ele. Din acest motiv pentru atacurile cibernetice e nevoie de atât de multă cercetare şi testare înainte ca războiul să izbucnească. Marile site-uri militare şi comerciale sunt de obicei reţelele reţelelor. Nu vei observa asta dacă intri pe un site mare să cumperi ceva, să scoţi ceva la licitaţie sau să te joci, dar vei vedea că majoritatea atacurilor de pe aceste site-uri nu le închid definitiv. Nu, un DDOS sau un

atac al viruşilor de obicei va încetini accesul pe un site mare. Asta pentru că site-ul a fost creat să facă faţă un atac puternic şi să meargă mai departe. Destul de ciudat, marile site-uri militare nu sunt la fel de bine echipate, în special pentru că Departamentul Apărării nu are atât de mulţi bani şi talent pentru a-şi construi site-urile mai puţin vulnerabile. Pentru un singur computer, nu poţi face multe cu această tehnică, din moment ce toate atacurile îţi vor lovi singurul computer. Dar e bine să ştii conceptul, cum reţelele de acasă sunt din ce în ce mai întâlnite, mai mulţi utilizatori vor considera folositor conceptul „fără şanse de eşuare”.

Mai sunt şi alte tehnici folosite de către cunoscători pe care le putem folosi şi noi. De exemplu, fii atent unde îţi păstrezi datele, pentru a nu-ţi fi furate. Poţi codifica paginile şi fişierele importante şi nu-ţi păstra parolele pe computer în acelaşi loc unde sunt datele.

Poate că cea mai mare greşeală a utilizatorilor {şi a multor afaceri mici) este arhiva stocată prost prin backup-ul datelor. Dacă un hacker îţi atacă serios sistemul, datele vor fi distruse sau deteriorate. Singurul mod de a evita acest lucru e să ai backupuri cu ce ai pe hard disk. Majoritatea utilizatorilor şi mulţi deţinători de afaceri mici nu se obosesc să facă asta. Cum toate hard disk-urile se strică la un moment dat, asta pare a fi o situaţie absurdă. Dar oamenii au refuzat să facă backupuri pentru că majoritatea au trecut la computere noi înainte ca cele vechi să cedeze. Fişierele sunt mutate de pe hard disk-ul vechi pe cel nou. Nu au fost suficiente poveşti cu utilizatori care-şi pierd tot conţinutul hard disk-ului ca să sperie oamenii să facă backupuri în mod regulat. Mai mult, sunt companii care vor recupera, pentru o sumă generoasă, datele de pe majoritatea hard disk-urilor care aparent sunt moarte. Ce trebuie învăţat de aici, dacă eşti vulnerabil în faţa unui atac al cyber-războiului, mai bine ţi-ai face backupuri de date în mod regulat. În ultimii câţiva ani,

cum tot mai mulţi oameni şi-au instalat drive-uri CD-RW, au început să le folosească exact cu acest scop. Dar realitatea e că, nici hard disk-urile predispuse la defecte, nici atacurile hackerilor nu există într-un număr aşa mare încât să-i facă pe oameni interesaţi de backup. Profesioniştii nu numai că fac backup în mod obişnuit (uneori chiar şi în fiecare minut), dar le şi păstrează timp de generaţii. Adică, există o copie de date separată pentru azi, pentru ieri şi uneori chiar de câteva zile (săptămâni sau luni). Aceasta va avea drept consecinţă poate zeci de copii ale aceloraşi fişiere. Dar dacă iei un virus agresiv, şi nu descoperi daunele câteva zile, va trebui să cauţi câteva generaţii de date ca să găseşti o copie bună.

Un alt mare avantaj pe care-l au site-urile profesionale militare şi comerciale este accesul la experţi în protecţia computerelor. În caz de urgenţă, un mic sfat inteligent poate conta mult. Acesta e unul din marile plusuri ale unui atac de succes asupra sistemelor de comunicaţie. Blochezi sistemul telefonic al unei ţări şi duşmanului tău îi va lua mai mult să-şi revină, pentru că experţii lor nu vor putea suna să vină cu soluţii. Ca utilizator obişnuit, poţi pune un bookmark la site-urile producătorilor de programe de protecţie şi programe software care acoperă de obicei securitatea internetului (www.cert. org e un loc bun de unde să începi, dar sunt şi alţii care să-ţi placă).

Site-urile bine protejate urmează o listă de reguli de bază cu ce au voie şi ce nu. Majoritatea nu se aplică computerelor personale (cum ar fi să nu dea voie adreselor de FTP anonime sau utilizatorilor să încarce fişiere pe serverul tău), dar unele da (cum ar fi folosirea unui program firewall dacă nu ai un modem pe cablu sau o conexiune DSL). FTP-ul anonim e o veche opţiune a internetului ce continuă să cauzeze probleme. Ea permite oricui să trimită un fişier serverului tău. Dar cineva cu instrumentele şi competenţele potrivite se poate folosi de

ele ca să intre pe serverul tău nu doar cu un fişier. Nu toate adresele anonime FTP sunt vulnerabile în faţa lor, dar sunt şi mulţi administratori de sistem conştienţi de pericol. De asemenea, sunt şi multe alte moduri de a trimite fişiere încolo şi-ncoace pe internet. Nu la fel de rapid ca FTP-ul, dar mai uşor de folosit, e HTTP, care se foloseşte pe majoritatea site-urilor.

Un alt obicei al marilor site-uri e acela de a înregistra toate operaţiunile. Acum, majoritatea utilizatorilor nu ştiu ce înseamnă asta, dar dacă foloseşti sisteme de operare ca Windows 2000 sau XP, trebuie să ai câteva programe de înregistrare funcţionale. Aceste operaţiuni înregistrează doar sarcini importante ale sistemului de operare pentru a fi folosite de tehnicienii de service (sau chiar pentru sistemul de operare) când repară ceva la sistemul tău. Dacă te apuci să cauţi în fişierele Help, poţi găsi unde sunt aceste înregistrări şi le poţi vedea. Un text anost, deşi poate surprinzător pentru că înregistrează operaţiunile eşuate care au fost detectate şi reparate fără să ştii. Deci, bun venit în secolul XXI. Marile site-uri fac asta deja şi înregistrează aproape totul. Aceste înregistrări deseori furnizează primul indiciu că site-ul a fost atacat, într-adevăr, hackerii vor vrea să aibă acces la înregistrări ca să-şi şteargă urmele.

Un alt instrument al profesioniştilor din ce în ce mai întâlnit la cei care au un singur computer e să fie la curent cu reparaţiile. Administratorii de sistem şi-au reparat software-ul sistemelor de operare cu sârguinţă ca să elimine („patch up”) defectele pe care hackerii le pot exploata ca să intre în sistem. E ceva nou în lumea computerelor până spre anii ’90, când administratorii de sistem îşi reparau sistemele de operare doar dacă era necesar. Nu de lene, ci din cauza faptului că reparaţiile aveau tendinţa să schimbe mai mult decât ce era defectat. După aplicarea reparaţiei, puteai descoperi că a creat noi erori, sau a schimbat modul de funcţionare a sistemului.

Schimbarea însemna mai multă muncă pentru administratorii de sistem şi mai multă nesiguranţă pentru utilizatori.

Dar asta s-a schimbat după apariţia World Wide Web şi explozia utilizării internetului. Această explozie însemna că mai multe computere erau expuse internetului şi atât ele, cât şi serverele puteau fi sparte. Computerele care funcţionau ca servere erau cele mai vulnerabile şi cele mai valoroase pentru hackeri (serverele păstrau deseori informaţii despre cardurile de credit). Dar până la sfârşitul anilor ’90, hackerii erau pe urmele utilizatorilor de internet. Acum era important pentru toţi să-şi facă reparaţiile la zi. Acum câţiva ani, majoritatea utilizatorilor nu ştiau ce înseamnă o reparaţie a software-ului şi dacă încercai să le explici, erau fie furioşi, fie le era frică, sau ambele. Furia şi frica sunt reale, dar şi cunoaşterea şi bunăvoinţa instalării reparaţiilor pentru software ar trebui să fie. Pentru că hackerii pot răspândi automat programe virus pe e-mail (şi prin vulnerabilul program Microsoft Outlook) unui număr mare de victime, mai mulţi oameni cunosc groaznicele consecinţe de „a nu avea cele mai noi reparaţii”.

Microsoft şi-a dat seama imediat că disponibilitatea şi nevoia de reparaţii nu-i făceau pe mulţi să-şi ţină software-ul updatat la zi. În mod normal, asta nu ar fi mare lucru. Mulţi oameni au folosit fără probleme software vechi de cinci sau zece ani, fără reparaţii. Dar cu cyber-războinicii care caută computere vulnerabile, fără reparaţii ca să stocheze programe zombie şi alte chestii, reducerea numărului de sisteme nereparate a devenit o problemă de securitate naţională. Aşa că Microsoft a ieşit pe piaţă cu „repararea automată” odată cu Windows XP în 2001. Erau câteva erori la el, bineînţeles, dar a redus numărul locurilor în care se puteau ascunde programele zombie.

Cel mai întâlnit punct slab al computerelor legate în reţea a fost din totdeauna parola. Băieţii răi fie le ghicesc,

fie le fură. Partea cu ghicitul a fost uşoară când spărgătorii creau programe-dicţionar. Acestea încercau să se logheze folosind o listă a celor mai des întâlnite parole şi, dacă niciuna nu mergea, treceau să-şi facă loc, literalmente, prin dicţionarul de cuvinte, apoi cuvinte şi numere. De fapt, genul acesta de lucruri pot fi combătute cu uşurinţă cu un software de logare care recunoaşte un „dictionary attack" (care necesită multe încercări ratate de logare din partea unui utilizator când sunt încercate parole diferite) şi suspendă utilizatorul până ce e verificată situaţia. Genul acesta de software de logare nu e unul obişnuit, aşa că dictionary attack-urile încă funcţionează. Totuşi, o parolă ce conţine un număr egal de litere şi numere va ţine dictionary attack-ul mergând până ce probabil va fi descoperit înainte de a reuşi să spargă parola.

În cazul sistemelor sigure, sunt alte moduri de a gestiona problemele protecţiei cu parolă. De exemplu, poţi avea un sistem call-back. Te loghezi, apoi eşti deconectat în timp ce sistemul pe care încerci să-l accesezi sună înapoi la un singur număr de telefon. Era o metodă des folosită înainte de apariţia internetului, dar funcţionează şi acum. Alte modalităţi foarte sigure sunt parolele folosite o singură dată (îţi faci o listă de parole şi o parcurgi, folosind o parolă după alta, secvenţial) şi două sau trei logări separate. Cu alte cuvinte, ai nevoie de o altă parolă pentru fiecare nivel. Au fost dezvoltate mult mai multe tehnici, dar problema principală, cea a furtului parolelor, rămâne. Soluţia biometrică începe să prindă contur. O „parolă" biometrică ar fi ceva de genul amprentei sau vocii. Şi acestea pot fi furate sau transmise, dar mult mai greu. E de la sine înţeles că fiecare organizaţie cyber-războinică are o divizie pentru spargerea parolelor şi depune eforturi să afle cum să intre în sistemele parolate inamice, dar şi să le apere pe ale lor.

Securitatea pe internet e o mare industrie şi ţara cu cea mai mare cotă a acestei industrii (Statele Unite) are,

tehnic, cel mai mare potenţial să treacă de orice program de protecţie. Într-adevăr, mulţi experţi din ţările străine cred că programele de securitate ce vin din Statele Unite vor avea intrări secrete care să permită cyber-războinicilor Departamentului Apărării să le acceseze pe timp de război, sau chiar în timp de pace, pentru spionaj economic. Asemenea căi de intrare sunt deseori ceva mai mult decât o parolă specială care nu poate fi schimbată niciodată. Nimeni nu va recunoaşte existenţa lor, dar ele există. Iar eforturile FBI de a impune legi ce forţează codarea sistemelor să aibă o intrare pentru ei, nu au făcut pe nimeni să se răzgândească. Partea bună e că paranoia intrărilor secrete va determina uneori guvernele străine să folosească software de protecţie inferioară.

Marele dezavantaj al Americii când vine vorba de securitatea pe internet e mărimea prezenţei sale. Majoritatea reţelei e în Statele Unite, ca şi cei mai mulţi utilizatori. Situaţia se schimbă, cum tot mai multă lume intră pe internet, dar vor fi întotdeauna mai multe site-uri şi utilizatori în Statele Unite decât altundeva. E mai mult de protejat, şi pentru că sunt mai mulţi inamici, dar şi mai multe ocazii de produce pagube. Departamentul Apărării a decis să folosească atât cantitatea, cât şi calitatea în construirea mecanismelor de securitate pe internet. Se folosesc mai multe nivele de protecţie. Acestea s-au dovedit a fi cel mai greu de penetrat atunci când „echipele de tigru” ale hackerilor prietenoşi sunt lăsate libere să încerce să intre.

Chiar mărimea resurselor de internet ale Americii face, virtual, imposibilă închiderea internetului Statelor Unite. Nu e cazul în multe alte ţări ca India, unde atacurile la scară largă pot închide internetul în ţară zile întregi, săptămâni sau luni.

La fel precum alte forme de război, când vine vorba de internet, cea mai bună apărare e atacul. Cum multe competiţii de hacking au arătat, nu există sistem ce nu

poate fi spart. Competiţiile de hacking oferă premii în bani celor care pot sparge un nou produs de protecţie într-o anumită perioadă de timp. Aceste competiţii sunt serioase. Oameni inteligenţi, competenţi şi dedicaţi au demonstrat în aceste competiţii cum se poate intra pe cel mai bine protejat sistem.

Totuşi trebuie reţinut încă un lucru: „nu contează cine e mai bun, ci cine e mai slab pregătit". Cei care lucrează cu cyber-războinici prost pregătiţi vor pierde.

PĂIANJENI TICĂLOŞI

Motoarele de căutare, acele site-uri foarte folositoare care ne permit să explorăm cyber-spaţiul, s-au dovedit a fi un alt defect pe internet. Lucru care demonstrează că punctele slabe pot apărea în cele mai neaşteptate locuri.

Folosind programe numite „spiders"1, acestea caută pe internet şi notează ce găsesc. Apoi clasează informaţia într-o bază de date. Utilizatorii motoarelor de căutare caută în acea bază de date atunci când folosesc aceste programe. Ani de zile, „păianjenii" nu au făcut decât să vadă dacă un site funcţiona şi notau ce găseau în baza de date a motorului de căutare. Totuşi, internetul înseamnă inovaţie şi progres. De exemplu, în 2001, motoarele de căutare începeau să verifice toate fişierele de pe site-uri {nu doar cele HTML sau paginile web, fişierele). Totul era spre bine, cum Adobe, fişierele de lucru, Power Point şi multe alte tipuri de fişiere erau verificate şi indexate. Puteai găsi acum informaţii utile cuprinse în acestea.

Din păcate, unele din aceste fişiere nu erau în mod normal accesibile navigatorilor pe internet şi cuprindeau informaţii pe care aceştia nu trebuiau să le vadă. Însă „păianjenii" puteau ajunge la ele şi adresele lor web intrau în indexul motorului de căutare. Imediat ce aveai adresa web, te puteai uita la ele. Gândeşte-te la webmasterii care pun parole sau fişiere cu informaţii despre cardurile de credit într-un loc în care toată lumea le poate vedea şi, ei

bine, avem o problemă. Acest lucru a fost iniţial observat când utilizatorii motoarelor de căutare raportau că au căutat „parola” şi au găsit fişiere care conţineau, ei bine, parolele utilizatorilor.

Singurul mod în care te puteai proteja de această problemă era să aduci problema în atenţia oricărui site pe care erau informaţii despre parolele şi cardurile de credit. Marile site-uri au fost primele care au observat problema şi au rezolvat-o. Cum am mai spus, asta se întâmplă pentru că ei au administratori profesionişti care să se ocupe de asta. Cel mai mult riscă site-urile afacerilor mici şi şcolilor care se susţin singure pe propriile servere. În aceste cazuri nu există cineva care să fie atent la problemele tehnice. Aici fişierele cu parole şi carduri de credit (sau informaţii personale) erau lăsate la îndemâna acestor motoare de căutare.

Această problemă nu e o situaţie unică. Internetul este o reţea atât de extinsă şi plină de diferite tipuri de software că nimeni nu ştie de fapt ce e vulnerabil şi la ce. Cel mai bine e să fiu atent şi pregătit să acţionezi repede. Pe internet, eşti fie rapid, fie mort. Acest incident arată că există multe situaţii periculoase care pot fi exploatate dacă exista circumstanţele propice.

ADWARE

Utilizatorii de internet au fost obişnuiţi să ia totul gratis de pe net. Din acest motiv sunt bannere şi reclame peste tot. Dar nu merg la fel de bine pe internet ca la radio sau la televizor – şi companiile de publicitate ştiu asta. Aşa că s-a venit cu o soluţie tehnologică menită să determine companiile de web să plătească şi să-şi menţină site-urile. Se numeşte publicitate targetată şi e procesul de identificare a utilizatorilor în funcţie de interesele lor şi postarea reclamelor la produsele pe care cel mai probabil aceştia le-ar cumpăra.

S-a ajuns astfel la folosirea a ceea ce s-a numit

„AdWare” sau, pentru necunoscători, „SpyWare”. AdWare-ul se descărca cu programe gratuite precum jocurile sau sistemele *de file sharing*. Odată instalat în sistem, navigarea pe internet era raportată unui site central unde preferinţele tale erau asociate profilelor publicitare ale posibililor clienţi. Aşa că, dacă intrai pe multe site-uri auto, vedeai mai multe reclame la maşini. Deşi SpyWare-ul nu colecta nimic personal în afară de preferinţele de navigare şi nu ştia nimic despre tine, mulţi oameni erau deranjaţi de acest sistem (deşi mai multora nu le păsa). SpyWare-ul trebuia să fie „Opţional” (folosit voluntar). Dar mulţi utilizatori nu citesc textul scris cu litere mici când descarcă un program gratis de la unele servicii online. Marea problemă cu SpyWare-ul este că funcţionează ca multe programe zombie ale hackerilor. Doar din cauza asta, mulţi utilizatori îşi curăţă computerul de SpyWare şi deseori descoperă că s-a furişat acolo. Chiar şi după îndepărtarea SpyWare-ului, nu e ceva neobişnuit să găseşti, când cauţi după o lună, că tot mai mulţi utilizatori au intrat în sistemul lor. Puţin înspăimântător, şi nu te aştepta ca aceste probleme să dispară. Şi apoi, câţi utilizatori ştiu de fapt ce programe sunt pe computerele lor?

HARDWARE ANTIC

Un avantaj pe care îl au oficialii militari (şi guvernamentali) ai Statelor Unite când au de a face cu hackerii black hat este vechimea computerelor şi software-ului cu care lucrează aceştia. În timp ce majoritatea firmelor civile îşi înlocuiesc computerele la doi-patru ani, armata şi guvernul le folosesc, câteodată, cam zece ani sau mai mult. Nu este aşa de rău pe cât pare. În primul rând, când vine vorba de multe sarcini de bază (cum ar fi procesarea de texte, paginile de lucru sau bazele de date), computerele care au zece ani încă pot face treaba bine. Cum organizaţiile militare şi guvernamentale nu au

niciodată atâtea computere de câte au nevoie, le păstrează pe cele vechi decât deloc. Totuşi, e nevoie de ingeniozitate şi de o vizită la halele de vechituri ca să găseşti componente de schimb pentru maşinăriile acestea vechi. Dar tot vei găsi multe din ele în depozitele bazelor militare şi birourilor guvernamentale. Până în 2000, FBI încă folosea multe computere 386 de la sfârşitul anilor ’80 (aveau doar *2%* din puterea unui computer de azi). Marea problemă a acestor computere vechi e că nu pot rula sisteme de operare şi noi browsere moderne. Aceste computere vechi nu pot, fără o mare greutate, să acceseze internetul (vechiul software de comunicaţii nu e compatibil cu internetul de azi şi browserele recente nu pot rula pe vechile 386 ale FBI). E încă posibil să poţi accesa cumva e-mailul cu maşinăriile acestea şi este interesant că marele avantaj e acela că aceste vechituri sunt mult mai puţin vulnerabile în faţa viruşilor dăunători şi viermilor ce împânzesc internetul. Literalmente, vechile computere nu pot rula viruşii moderni pentru că nu au capacităţile cerute.

Un aspect militar e că multe ţări mai puţin bogate au echipament PC vechi. A existat dintotdeauna o piaţă activă a computerelor vechi în părţi precum America de Sud, Africa şi Asia. Multe armate şi grupări de rebeli din aceste zone au echipamente vechi şi imunitate la instrumente moderne de hacking pe care computerele scoase din uz le lasă în spate. Mai vechi înseamnă uneori şi mai bun, iar cyber-războinicii sunt gata pentru asta.

SOLUŢII NOI

De frica terorismului pe internet, puţini, dacă nu niciunul, oameni au fost ucişi prin intermediul acestei reţele. Cel puţin nu încă. Dar ceva atât de imens, care ajunge în atât de multe locuinţe şi locuri de muncă şi consumă vieţile oamenilor aşa de mult, totuşi, trebuia să inspire o oarecare frică. În realitate, majoritatea

dezavantajelor internetului sunt neplăceri, nu dezastre. Pierderea unor fişiere importante pentru afacerea ta din cauza unui virus (sau lipsa copiilor de rezervă) e un dezastru. Să te lupţi cu toţi script kiddies de peste tot, frica de viruşi, nesfârşite reparaţii de software, necazurile cu software-ul antivirus şi backup-urile sunt o neplăcere. Dar va fi o şi mai mare neplăcere dacă problemele nu vor fi rezolvate, iar teama ca teroriştii pot transforma neplăcerile în dezastre determină încercări serioase de a schimba situaţia. Un motiv pentru care Microsoft şi-a anunţat public noua atitudine cu privire la erorile de software şi punctele slabe ale sistemului de protecţie (vor fi mult mai puţine) este acţiunea legislatorilor care făceau gălăgie în privinţa legilor care-i obligau pe producătorii de software să fie responsabili de daunele cauzate de defectele din programele lor. Nu e o idee nouă, dar până în 2001 (din cauza unei creşteri acute a punctelor slabe ale internetului şi a războiului împotriva terorismului), producătorii de software au putut evita problema. Au existat câteva încercări de a-i face responsabili în timpul anilor ’80, căci un număr de utilizatori a reclamat un software infectat. Printr-o eschivare elegantă („E vorba doar despre computere, noi suntem companii mici”), şi o atitudine orientată spre afaceri dublată de promisiuni că va fi mai bine, au blocat toate plângerile. În ultimii zece ani, producătorii de software au obţinut condiţii mai bune pentru ei, sub masca ajutorului oferit în eradicarea pirateriei software-ului. E o situaţie destul de bună pentru producătorii software-ului de computer. Multe programe nu sunt foarte bune, dar sistemul legislativ descurajează cu entuziasm orice acţiune legală împotriva producătorilor. Dar cu toate problemele internetului, multe dintre ele au dus direct spre produsele Microsoft, iar legislaţia în vigoare e pusă în discuţie. Acest aspect îi sperie pe producătorii de software mult, şi aşa şi trebuie. Toate acele procese ar fi scumpe şi chiar dacă multe din ele nu aveau o

bază, publicitatea negativă le-ar face la fel de mult rău. Deci e destul de probabil ca producătorii să îmbunătăţească controlul calităţii de acum încolo.

Totuşi, sunt şi câteva părţi negative asociate cu crearea de software mai bun. O lege care ar fi pe placul producătorilor este una care să reglementeze modul în care erorile de software, mai ales cele legate de internet, sunt raportate. Potrivit legilor propuse, oricui găseşte o eroare i se cere prin lege să o raporteze imediat agenţiei federale apropiate sau producătorului. Publicarea erorii, mai ales pe internet, ar fi o infracţiune. Motivul din spatele acestui demers e să-i împiedice pe băieţii răi să le exploateze înainte ca producătorii să le poată repara. Reversul medaliei e că majoritatea oamenilor cred că erorile ascunse vor permite producătorilor să ignore o parte din ele şi să dureze o perioadă mare de timp până le repară pe celelalte. Majoritatea utilizatorilor cred că un producător de software care spune: „Ai încredere în mine”, ei bine, nu e de crezut.

Producătorii de software pot vedea că ameninţarea cu cyber-războiul poate fi posibilă prin erorile din programele lor. Frica e un factor motivator şi când vine vorba de cyber-război sunt multe de care să ne temem.

LUCRURI IMPORTANTE DE FĂCUT

Dacă ai fost lovit de un virus precum „I Love You”, „Melissa”, „Code Red” sau „Nimba”, înseamnă că eşti deja o victimă a unei dispute cyber-războinice. Probabil ai fost victimă chiar de mai multe ori, pentru că, dacă ai fost online şi ai observat că internetul pare „leneş”, este foarte posibil ca acest lucru să se fi întâmplat pentru că cineva din vecinătate a fost lovit de un atac DDOS major. Va încetini şi din viteza de internet a membrilor din reţea. Există şi alte metode de a fi atacat pe internet. A fost furat vreun număr de card de credit de pe site-ul web pe care îl deţii? Este o altă aventură neplăcută, dar comună pentru

utilizatorii de internet.

Nu eşti paranoic dacă ai impresia că lucrurile se vor înrăutăţi şi mai tare. Cyber-războiul nu are nevoie de cineva care să creeze arme. Nu e nevoie decât de câteva sute de oameni care să fie dispuşi să facă munca murdară şi o bibliotecă cu trucuri meschine pe care nimeni nu le-a mai văzut până acum. Un cyber-război major, „Cel Mare”, te-ar putea scoate de pe internet timp de mai multe zile sau săptămâni sau îţi poate şterge totul de pe hard.

Aşadar, cum să te protejezi? Există metode pentru a face asta.

Fii atent! Şi în timp ce faci asta, salvează www.cert.org, site-ul web care va avea întotdeauna cele mai noi informaţii despre securitatea pe internet. Site-ul CERT (Computer Emergency Response Team) este unul dintre cele câteva care pot fi folosite ca un loc unde merită să te opreşti pentru a afla ce se mai întâmplă în domeniul securităţii pe internet.

Mai jos sunt remedii specifice. Ele sunt enumerate în ordinea importanţei (cele mai importante sunt primele). Fac acest lucru pentru a evidenţia că deşi sunt multe căi prin care un hacker poate ajunge în PC-ul tău, realitatea este că atacurile hackerilor sunt rare. Cele mai comune probleme cu hackerii sunt acei viruşi care se răspândesc automat din cauza erorilor din Microsoft Windows (mai ales scriptingul care este folosit în programul lor de e-mail Outlook). Aşadar, din cele 11 puncte enumerate mai jos, primele trei îţi vor oferi cea mai bună protecţie. Alege nivelul de securitate care ţi se potriveşte cel mai bine.

1. Dacă foloseşti un software Microsoft, mai ales programul de e-mail Outlook (sau Outlook Express), opreşte scriptingul. Nu este un lucru uşor de făcut, mai ales cu toate acele sisteme de operare Microsoft diferite. Pentru a afla cum să faci asta, orice versiune de Outlook ai avea, mergi la www.microsoft.com şi caută acolo opţiunea

Disable scripting. Va apărea un document cu ce trebuie să faci în cazul computerului tău.

2. Nu face nimic cu un fişier ataşat dacă nu ştii ce este, nu îl aşteptai sau este de la cineva pe care nu îl cunoşti. Chiar dacă primeşti unul din acele fişiere cu „lucruri amuzante” (imagini, programe sau documente) pe care oamenii le dau mai departe; aşteaptă o zi sau două înainte de a-l deschide. Lasă pe altcineva să fie lovit sau să dea alarma. Dacă ai oprită macroexecuţia pentru Word sau fişiere Excel, poţi deschide aceste documente în siguranţă. Dar este mai bine să fii cu capul pe umeri. Dacă nu ştii de unde a venit un fişier, află. Dacă nu poţi, şterge-l. Nu e mare pierdere.

3. Dacă foloseşti Microsoft Office şi vrei să eviţi macroviruşii, închide execuţia macro. Dacă foloseşti Word 97, poţi face asta dacă mergi cu mouse-ul la Tools/Options/General şi bifezi „Macro virus protection”. În Word 2000 se face diferit. Apasă pe Tools/Macro/Security şi alege High. De fapt, acest lucru închide execuţia macro. Dacă ai o altă versiune de Word, mergi la www.microsoft.com şi caută „disable macros”. Aceeaşi procedură este folosită pentru foile de lucru din Excel. Deşi nu sunt la fel de mult răspândiţi sau la fel de mortali ca viruşii, cei macro (puşi în funcţiune atunci când deschizi documentul) există din 1995 (pentru Word, 1996 pentru Excel).

4. Fii atent când descarci fişiere! Dacă este posibil, descarcă numai materiale de pe site-uri cu o bună reputaţie. Încă mai există foarte multe programe infestate (cu viruşi şi alte programe distructive) pe internet. „Site-urile cu bună reputaţie” sunt cele care aparţin companiilor importante sau unor oameni pe care îi cunoşti. Cei care conduc site-ul dau reputaţie şi siguranţă acestuia. Înainte de a le face disponibile, aceştia vor trece toate programele descărcabile şi fişierele printr-un program antivirus. Site-urile mult mai mici nu fac acest lucru şi acesta este un

motiv pentru care viruşii rămân în circulaţie.

5. Multe dintre vulnerabilităţile în faţa viruşilor sunt reparate cu actualizări ale sistemului sau ale software-ului. Pe măsură ce sunt descoperite erori în acest software, producătorii pregătesc programe gratuite pe care le poţi descărca şi rula pentru a „petici" software-ul. Sistemul tău de operare şi programele de software importante au informaţii în sistemele Help" despre locul de unde poţi lua actualizări. Multe versiuni recente de software vor folosi şi o conexiune la internet disponibilă pentru a se actualiza automat. Software-ul AOL face acest lucru de ani de zile.

6. Un alt element util pentru securitate este un program antivirus. Acesta se încarcă de obicei atunci când dai drumul la computer şi caută viruşi (şi alte software-uri cu probleme) pe care îi elimină atunci când îi găseşte. Instalarea unui software antivirus care să ruleze în permanenţă pe computer poate destabiliza uneori sistemul şi poate crea probleme atunci când descarci materiale de pe web sau încerci să instalezi un software nou. Nu uita, totuşi, că dacă nu ai un firewall şi foloseşti software Microsoft, există erori în acesta care îi pot permite unui hacker să pătrundă în computerul tău fără să folosească un virus de e-mail sau un document macro. De fapt, dacă ai grijă de unde iei fişierele şi ataşamentele de e-mail de pe internet sau ce pui în PC-ul tău, poţi rula programul antivirus doar o dată pe lună. Când rulezi software-ul anti virus, asigură-te că are cea mai nouă bază de date cu viruşii cunoscuţi. Nu trebuie decât să fii online. Aşa ca verifică informaţiile despre antivirus. Pentru soluţii, mergi la orice motor de căutare şi tastează „antivirus software" (cu ghilimele) şi îţi vor fi arătate cele mai noi software – un de apărare. Este un domeniu care evoluează rapid, aşa că este mai sigur să laşi un motor de căutare să te ducă la cele mai noi versiuni de software antivirus disponibile.

7. Asigură-te că ai oprit transferul de fişiere. Această opţiune (pe sistemele de operare Microsoft) este găsită fie

la Network Properties, fie la Properties şi se numeşte Sharing pentru segmentul de stocare. Nu ai nevoie de transferul de fişiere dacă nu eşti pe o reţea locală. Computerele personale au de multe ori transferul de fişiere pornit (din greşeală, de obicei, atunci când cineva se joacă cu setările computerului) şi singurul mod în care poate fi folosit este dacă un hacker intră pe PC-ul tău.

8. Nu este o idee rea să renunţi la Outlook (cel puţin pentru e-mail, calendarul/orarul nu sunt nici pe jumătate la fel de rele). Există Eudora (www.eudora.com), care este mai vechi pe piaţă şi mai sigur decât Outlook. Eudora (şi multe produse similare) va înlocui cu uşurinţă Outlook-ul. Dacă eşti utilizator AOL, deja eşti mai în siguranţă. Spre deosebire de Outlook, foarte puţini viruşi sunt creaţi pentru a ataca utilizatori ai programului de e-mail AOL. Deşi AOL are peste 30 de milioane de utilizatori, sunt aproape de zece ori mai mulţi oameni care folosesc alte ISP-uri pentru a intra pe net. Şi cei mai mulţi dintre aceştia folosesc software-ul Microsoft. Mai mult, AOL şi Eudora (şi alte programe de e-mail decât cele Microsoft) sunt construite cu o mare atenţie pentru securitate. Aşa că hackerii au două motive să atace ţintele Outlook: Microsoft produce un software mai vulnerabil şi există mult mai multe vulnerabilităţi de sistem.

9. Parolele au fost întotdeauna cea mai mare problemă de securitate a computerelor şi cea mai mare vulnerabilitate pe (sau în afara) internet. Ar trebui să îţi schimbi parola des şi să foloseşti unele greu de dezlegat de instrumentele hackerilor. Aceasta înseamnă o combinaţie greu de ţinut minte de cel puţin opt litere şi cifre.

Din motive practice, cei mai mulţi oameni nu vor pune o parolă greu de reţinut atunci când au de ales. De aceea, în multe organizaţii, vezi foarte multe bileţele cu parole scrise, lipite de ecranul computerului. Ajutorul este pe drum sub forma biometricii, o tehnică ce foloseşte lucruri precum amprentele, forma feţei sau chiar „pumnul”

(modul în care loveşti tastatura) pentru a te identifica. Dar între timp, „gândeşte diferit” când e vorba despre inventarea parolelor.

10. Nu folosi întotdeauna opţiunea „save password” pentru programe şi site-uri web. Deşi această opţiune îţi economiseşte timp în viitor (nu mai trebuie să introduci parola), dar este posibil ca hackerii să citească aceste parole din listele salvate în fişierele ascunse de pe hard. Aşadar, parolele pentru lucruri precum banca sau conturile la bursă nu ar trebui salvate pe hard, cu toate că probabil nu va fi necesar să introduci astfel de date pe site-uri web. Nu te va costa nimic dacă cineva ia parolele pentru nişte site-uri de ştiri sau de divertisment.

11. Nu stoca informaţii despre cardul de credit sau contul bancar online sau informaţii despre bursă pe computerul tău. Dacă vei păstra o lista cu informaţii despre cardul de credit pe computer, nu o lăsa pe hard, ci copiaz-o pe un dispozitiv pe care să-l păstrezi în altă parte. Cele mai mari instituţii financiare au o mai bună securitate pentru internet decât media celor folosite acasă. Dacă cineva îţi sparge computerul de acasă, va căuta parole şi informaţii despre cardul de credit. Dacă, trebuie să salvezi astfel de informaţii pe computer, foloseşte fişiere criptate. Sistemele de operare Microsoft precum NT, 2000 şi XP suportă toate acestea şi sunt programe disponibile pentru sistemele de operare care nu au criptarea încorporată. Dacă cineva îţi sparge sistemul, este posibil să treacă de codarea ta, dar oferă un grad în plus de protecţie. Ca să găseşti software pentru criptarea fişierelor de pe hard, mergi la un motor de căutare (precum google.com) şi tastează „encrypted folders” (cu ghilimele) şi îţi vor apărea cele mai noi produse disponibile. Unele pot fi gratuite, celelalte vor fi ieftine.

PENTRU UTILIZATORII DE MODEM PRIN CABLU ŞI DSL

Dacă ai o conexiune rapidă şi mereu activă (modem prin cablu sau DSL), ai nevoie de un program firewall. Fără un firewall, eşti momeală sigură pentru hackeri. Când foloseai un modem prin telefon erai protejat de mulţi hackeri pentru că exista o nouă adresă de internet (IP) de fiecare dată când te conectai. Dar cu o conexiune „mereu activă" ai propria adresă permanentă de la furnizorul de internet (prin cablu sau companie telefonică). Astfel, unui hacker îi este mai uşor să te găsească. Dar cel mai important pentru hacker este faptul că ai o conexiune rapidă. Astfel pot fi produse mai multe pagube celorlalţi prin folosirea câtorva metode de atac. Cum PC-ul tău este mereu conectat, sunt mai multe şanse să fiu detectat de hackeri care scanează netul pentru locuri unde să îşi parcheze armele sau etapele intermediare pentru proiecte mai ambiţioase. Un program firewall nu va opri un hacker cu adevărat determinat, deşi poate încetini orice încercare de spargere de pe sistemul tău. De asemenea, un firewall acţionează (la propriu) ca un sistem de alarmă împotriva infractorilor. Acest lucru îi va face pe cei mai mulţi dintre hackeri să se mute către o ţintă mai puţin protejată. Singurul mare sistem de operare care are un astfel de program inclus este Windows XP. Poţi găsi programe firewall în cele mai multe magazine software. Online, mergi la un motor de căutare şi tastează „firewall programs" şi vei vedea câteva disponibile, la fel ca şi discuţii între utilizatori şi modul de folosire. Sunt câteva firewall-uri bune disponibile gratuit (numai pentru utilizare de acasă). La început pot crea confuzie şi par greu de folosit. Eşti întrebat dacă accepţi sau refuzi să fii contactat de multe surse de care nu ai auzit niciodată. Toate au sens dacă eşti un expert în internet, dar pentru cei mai mulţi dintre oameni este un pic şocant. Din fericire, poţi răspunde cu un la toate acele întrebări dacă laşi pe cineva să intre sau să iasă şi îţi vei da seama despre ce este vorba din încercări şi greşeli. Acesta este preţul securităţii. Până

la sfârşitul deceniului, cea mai mare parte din problemele de utilizare a firewall-urilor vor fi probabil rezolvate. Competiţia face asta şi nu uita ca în cele din urmă (poate în cinci-zece ani) securitatea de pe internet se va întări destul de mult. Multe dintre software-urile pentru internet acordă mult mai multă atenţie securităţii. Dar între timp, poţi fi expus riscului. Dacă tot vorbim despre asta, ar trebui evidenţiat că numai o parte foarte mică din utilizatorii de PC-uri cu o conexiune rapidă vor fi folosiţi pentru un atac cibernetic. Numai câteva mii de PC-uri, cel mult, vor fi necesare pentru o asemenea operaţiune. Adică mai puţin de un PC cu o conexiune rapidă dintr-o mie. Dar hackerul poate decide că distrugerea datelor de pe majoritatea PC-urilor cu o conexiune rapidă din SUA poate avea valoare militară. Acest lucru ar putea fi făcut cu câţiva viruşi obişnuiţi.

UTILIZATORII UNIX/LINUX

Următoarele sfaturi sunt pentru utilizatorii de Unix sau Linux. Dacă nu eşti unul dintre ei, poţi sări peste această parte. Şi utilizatorii Unix sau Linux sunt atacaţi, dar nu la fel de mult ca sistemele Microsoft. Chiar şi aşa, sunt lucruri pe care le poţi face pentru a-ţi minimaliza vulnerabilitatea. De exemplu, nu folosi rutenii decât dacă este absolut necesar. Mai exact, nu rula programe precum X Windows sau aplicaţii precum IRC. Hackerilor le este mai uşor să pătrundă în aceste programe şi odată ce au făcut-o au capacitatea de a face mai multe pagube. De asemenea, asigură-te că eşti protejat, închide toate serviciile de care nu ai nevoie şi păstrează copiile. Acest avertisment se aplică în mod special utilizatorilor de Linux. Unix este de multă vreme sistemul de operare pentru profesionişti. Dar Linux ţinteşte acum un segment de piaţă. Deşi Linux (şi Unix) prezintă mai multă siguranţă decât sistemele de operare Microsoft, tot mai există pericole.

Nu uita că, oricât de bun ar fi sistemul de operare,

orice server sau PC poate fi spart dacă atacatorul este bine pregătit şi suficient de insistent. Script kiddies şi hackerii black hat tind să evite PC-urile care par să aibă un anumit grad de protecţie. Dar în cele mai multe cazuri, un atac de succes înseamnă nişte puşti care caută un loc de parcare pentru zombie, colecţia de pornografie sau filme furate ori informaţii despre carduri de credit. De asemenea, există şansa ca PC-ul tău spart să fie preluat de nişte cyber-soldaţi sau cyber-terorişti din Orientul Mijlociu care caută un loc de unde să îşi lanseze atacurile cyber-războinice. Aşadar, opune puţină rezistenţă şi vor pleca să caute un loc mai accesibil. E ca bancul despre ce faci atunci când tu şi prietenul tău vă întâlniţi cu un urs nervos. Urşii pot alerga mai repede decât orice om. Dar pentru a scăpa în această situaţie, nu trebuie să alergi mai repede decât ursul, ci doar mai repede decât prietenul tău.

NU-ŢI FACE GRIJI, FII FERICIT!

Dacă faci tot ce este rezonabil posibil pentru a-ţi menţine PC-ul în siguranţă, nu are rost să te superi dacă un atac informatic te loveşte oricum. Pentru ca orice ar ajunge la tine în aceste împrejurări, probabil loveşte o mulţime de alţi oameni şi site-uri web mult mai rău. Acest lucru, cel puţin, pune presiune asupra mai multor oameni să facă ceva (ce tu ai făcut probabil deja). Unul dintre adevărurile fundamentale despre internet este acela că este relativ uşor să te aperi. Dar pentru că mulţi oameni nu iau tehnologia foarte în serios, deşi există motiv pentru care ar trebui să o facă, devin vulnerabili în faţa atacurilor pe internet. Producătorii de PC-uri şi software-uri şi-au dat seama de multă vreme că nu pot vinde o cantitate mare de hardware şi software dacă PC-ul nu este la fel de uşor de folosit ca un cuptor de pâine. OK, poate că este un pic exagerat. Dar producătorii de aparate video au învăţat de-a lungul anilor că funcţiile lor de programare banale îi zăpăceau pe cei mai mulţi utilizatori. Producătorii de PC-

uri au adoptat foarte repede, ca martori ai succesului, conceptul prezentat de MacIntosh şi Windows, „Point and click”. Din păcate, nimeni nu a putut reglementa internetul în primele sale etape de dezvoltare pentru a impune o securitate puternică. Una dintre marile dezbateri dintre utilizatorii de internet este nevoia unei reforme în privinţa conducerii internetului şi a software-ului său. Este foarte realităţilor să asistăm la naşterea unui nou internet, unul care va face faţă lucrurilor precum spamurile, securitatea şi apărarea împotriva agresorilor care eliberează viruşi doar pentru a vedea ce pagube pot crea. Ajutorul va veni cu siguranţă şi merită să-i aştepţi dacă îţi iei unele măsuri de precauţie (din cele enumerate mai sus).

ANEXE

FORŢELE AERIENE AMERICANE ŞI CYBER-RĂZBOIUL

În anul 2001, forţele aeriene ale Statelor Unite s-au plâns că, după un deceniu în care bugetul pentru apărare a fost redus, a apărut o altă problemă ce trebuia rezolvată: personalul îmbătrânit. Problema în sine este discutabilă din moment ce forţele aeriene creează şi construiesc avioane pentru a concura cu inamici care nu mai există. Cu toate acestea, forţele aeriene au vrut minimum 20 de miliarde de dolari în plus pe an pentru a face faţă deficitului de şapte miliarde de dolari pe an (sau mai mult) începând din 2002. Ceea ce a dus la acest deficit a fost dorinţa forţelor aeriene de a da curs unor forme netradiţionale de război, în special război informaţional. Aici sunt incluse bazele de război ale internetului, loc în care forţele aeriene au activat pe parcursul anilor ’90. Într-adevăr, forţele aeriene au avut atât de mult succes cu eforturile pentru războiul informaţional încât şi-au pierdut cei mai talentaţi cyber-războinici, care au ales cariere civile mai profitabile. Ei bine, forţele aeriene nu îi pierd în totalitate pe aceşti aşi ai războiului informaţional şi pot, ceea ce şi fac de multe ori, să îi angajeze din nou în calitate de contractori civili (de multe ori la acelaşi preţ cu care îi plăteau atunci când erau ofiţeri ai forţelor aeriene).

Războiul din Afganistan şi războiul împotriva terorismului au rezolvat problemele bugetare ale forţelor aeriene. Deşi pot cumpăra cu sume mari de bani lucruri de care nu au cu adevărat nevoie, banii cheltuiţi pentru cyber-război sunt bine folosiţi. Nu uita că, în anul 2002, guvernul Statelor Unite a cheltuit 44, 9 miliarde de dolari pe computere, software şi reţele. Jumătate din această sumă a fost folosită de Departamentul Apărării. Aproape jumătate din aceşti bani au fost cheltuiţi sau controlaţi de forţele aeriene. Declaraţiile lor ţin loc de explicaţii:

Declaraţie făcută de către generalul-locotenent John L. Woodward Jr., USAF Purtător de cuvânt, Comunicaţii şi informaţii, Securitatea informaţiilor.

Transcrierea discursului ţinut în faţa Comitetului Serviciilor Armate în data de 17 mai 2001.

Domnule preşedinte, stimaţi membri ai comitetului, vă mulţumesc pentru interesul continuu de care aţi dat dovadă în această problemă naţionala foarte importantă. Aceasta este cea de-a patra oportunitate a forţelor aeriene de a-şi exprima punctul de vedere în legătură cu acest subiect. Cu susţinerea Congresului, eforturile noastre din ultimii patru ani au continuat să întărească protecţia reţelelor noastre. Ca forţă aero-spaţială, informaţiile şi luarea deciziilor rămân puncte critice pentru securitatea mondială. După cum şeful personalului forţelor aeriene, generalul Ryan, spune, „sistemele noastre de informaţii şi reţelele merg la război cu noi şi, pentru că fac parte din luptă, trebuie să le tratăm ca pe nişte sisteme armate”.

În 1997, a început procesul de construire a unei reţele puternice pe măsură ce doctrina lor a fost stabilirea superiorităţii informaţiei ca armă fundamentală în orice război. La acea vreme, existau planuri de a furniza fiecărei baze a forţelor aeriene un sistem de detectare a intruziunilor. Deşi am început să instalăm sisteme de tip firewall, ele erau excepţia. Pe lângă proiectarea centrelor de control ale reţelelor, am dezvoltat un concept de securitate, de apărare, cunoscut sub numele de Barner Reef la care echipele noastre de specialişti lucrează deja de patru ani.

În 1998, cu ajutorul susţinerii financiare a Congresului, am dus la bun sfârşit un program accelerat de instalare a unei suite de capacităţi de manageriere a reţelelor şi a unor instrumente de protecţie a informaţiilor (NMS/BIP) în 109 baze. De asemenea, am instalat sisteme de tip firewall, instrumente de scanare şi instrumente de manageriere a reţelelor în bazele principale. Conceptul

nostru de „operaţionalizare şi profesionalizare a reţelelor” este în plină desfăşurare; cu alte cuvinte, tratăm reţelele ca pe nişte sisteme armate, ceea ce au şi devenit de fapt.

Pentru a maximiza eficienţa reţelelor noastre mobile şi pentru fi siguri că le putem controla corespunzător, instrumentele folosite în comunicaţii (pachetele mobile de comunicaţii de război) oglindesc instrumentele cele mai importante din bazele fixe.

În 1999, AFCERT a căpătat o importanţă vitală în forţele de comando pentru apărarea reţelelor de calculator şi am publicat doctrina operaţiunilor informaţionale. Fiecare bază a forţelor aeriene avea un centru de control al reţelelor cu un set iniţial de instrumente pentru protecţia reţelelor şi am început să înfiinţăm centre de securitate în cadrul comandamentelor majore. După operaţiunea DESERT FOX ne-am consolidat sistemele de protecţie întrucât încercările de intruziune în reţelele bazelor au continuat să crească.

În anul 2000, sistemele de detectare a intruziunilor apărau fiecare bază operaţională, scanând în mod activ reţelele în căutarea activităţilor maliţioase sau a vulnerabilităţilor. Am actualizat seturile de instrumente pentru protecţia informaţiilor şi am însărcinat centrele de control al reţelelor să raporteze scanările, la fel ca în cadrul oricărui sistem de arme, prin sistemul de instruire şi verificarea resurselor. Conducem un sistem la nivel mondial, reţeaua noastră, dar ameninţările la adresa ei sunt reale şi periculoase. Operaţiunea ALLIED FORCE a testat iniţiativa noastră şi am fost martori la ceea ce mulţi numesc primul efort „Cyber-războinic”.

În declaraţia mea de azi, mă voi concentra pe succesele operaţionale care ţin de securitatea informaţiilor, mediul online în care lucrăm şi modul în care au progresat în această direcţie.

Succese operaţionale

Forţele aeriene au adoptat şi au pus în practică un concept interesant numit „One Air Force – One Network” 1. Conceptul funcţionează în cadrul unei companii sau într-un mediu corporatist şi valorifică cele mai bune servicii ale întreprinderii. Forţele aeriene echilibrează puterea netului şi o pun la dispoziţia fiecărui membru al lor. De fapt, continuăm să echilibrăm informaţiile pentru succesul în luptă, chiar dacă reţelele noastre de comunicaţii sunt supuse în mod repetat testărilor, blocării e-mailurilor, unui program de genul

„Virusul săptămânii”. Totuşi, operaţiunile pe care le desfăşurăm continuă neafectate.

Daţi-mi voie să ilustrez cu câteva exemple:

— Compania noastră de informaţii a interceptat peste 315 milioane de încercări de conexiune suspecte anul trecut la reţeaua noastră de senzori, ceea ce a dus la o medie de o conexiune neautorizată din exterior la fiecare 20 de milioane de încercări de conectare suspecte. În total, impactul a fost nesemnificativ. Aceasta ţine de securitatea informaţiilor.

— Forţele aeriene au ridicat de curând standardele INFOCON la un nivel mai înalt din cauza activităţii de hacking căreia i s-a făcut reclamă în urma incidentului EP-3. Am combătut cu succes acţiunile tot mai dese de hacking împotriva capacităţilor misiunii noastre.

— Un rol critic pentru succesul oricărei misiuni îl are Teatrul de Desfăşurare al Comunicaţiilor (TDC) menţionat mai devreme. Până azi, am folosit mai mult de 33 de terminale de sateliţi cu bandă multiplă ce furnizează o bună capacitate de răspuns la mare distanţă. Pachetul nostru integrat de acces la comunicaţii care oferă o infostructură a bazelor mobile, similară bazelor fixe de comunicaţii a fost certificat pentru interoperabilitate.

— Conceptul de recepţie continuă să funcţioneze bine pentru misiunile noastre globale. Sistemele noastre de informaţii, care conţin atât echipamente de comunicare

comerciale, cât şi militare, au permis un răspuns prompt şi sigur pentru informaţiile secrete, logistica şi susţinerea oamenilor din SUA; în caz contrar, am fi fost nevoiţi să apelăm la forţele de comando din sud-vestul Asiei.

— Şi răspunsul nostru în faţa ameninţărilor cu viruşi a fost îmbunătăţit, în trecutul apropiat, viruşii „I Love You" şi „Melissa" au infectat e-mailurile ce au fost deschise de mulţi utilizatori. Azi, în urma pregătirilor, a cunoştinţelor şi a procedurilor, e-mailurile afectate de viruşi precum „Naked Wife" sau „Anna Kournikova" nu au mai fost deschise.

În ciuda succeselor noastre, nu putem subestima pericolele care ne pândesc în era informaţională. Doar pentru că nu am avut multe probleme de apărare nu înseamnă că suntem protejaţi de atacul cibernetic.

Atacurile cibernetice pe care continuăm să le experimentăm sunt reale şi periculoase. În analizele finale, situaţia securităţii informaţiilor ne-a asigurat că atacurile cibernetice nu sunt decât o neplăcere cu un impact neînsemnat asupra operaţiunilor de luptă, dar trebuie să continuăm să învăţăm şi să ne îmbunătăţim procedurile pentru a fi întotdeauna cu un pas înaintea ameninţării lor.

Mediul informaţional al companiilor şi poziţia forţelor aeriene.

Ameninţările puternice şi sofisticate continuă să evolueze, obligându-ne să menţinem menţinem o poziţie de superioritate informaţională. Muncim pentru a face faţă acestor provocări printr-o strategie de apărare în profunzime care integrează capacităţile oamenilor, operaţiunile şi tehnologia. Prin această strategie ne asigurăm că transmitem informaţii corecte luptătorului, în orice moment şi în orice loc. Politica noastră este că securitatea e o problemă care priveşte pe toată lumea şi până la proba contrarie tratăm fiecare incident ca pe un potenţial atac. Până în acel moment, suntem agresivi în folosirea programelor de apărare şi recunoaştere.

— Pentru a sublinia că securitatea informaţiilor este o responsabilitate a fiecărui membru al forţelor aeriene, s-a iniţiat de la centru o campanie de implementare şi recunoaştere cu o durată de un an, care a început în ianuarie 2001. Fiind o campanie ce se adresa tuturor militarilor noştri, fiecare comandant şi agenţie a forţelor aeriene sponsorizează timp de o lună şi dezvoltă un anumit program care va fi folosit de toţi ceilalţi. Campania este creată pentru a câştiga bătălii şi războaie asigurându-se că toţi utilizatorii sunt conştienţi de acest lucru şi îşi iau în serios responsabilităţile de securizare a informaţiilor.

— Comandanţii sunt implicaţi la toate nivelurile pentru a menţine recunoaşterea tuturor ameninţărilor şi atacurilor împotriva reţelelor noastre. Am stabilit puncte de reper ferme, pentru implementarea INFOCON care se asigură că toţi comandanţii noştri sunt permanent în temă şi pregătiţi pentru atacuri împotriva reţelelor. Mai mult, forţele aeriene modifică procesul operaţional deraportare şi cer acum rapoarte obligatorii pentru toate incidentele de acces informatic neautorizat.

Forţele aeriene se implică atent în procesul de alertă de vulnerabilitate a securităţii informaţionale şi îl îmbunătăţeşte folosind sistemul Time Compliance Network Order. Eforturile noastre asigură faptul că vulnerabilităţile sunt identificate şi riscurile sunt micşorate prin securizarea reţelelor şi folosind un sistem de raportare a comenzilor şi controlului folosit la toate nivelurile şi uşor de verificat.

CERT este cea de a 33-a divizie de operaţiuni informaţionale a forţelor aeriene. În punctul culminant al oricărei bătălii cibernetice, războinicii noştri din prima linie sunt profesioniştii în comunicare ai operaţiunilor de reţea coordonate de Comandamentul Central, ai centrelor de securitate şi de control al reţelelor. Împreună monitorizează reţelele forţelor aeriene în timp real pentru a identifica activităţile maliţioase. CERT va conduce în

sens invers acţiunile de apărare şi va iniţia canale de raportare către reţelele forţelor de comando. De asemenea, sunt responsabili de identificarea vulnerabilităţilor reţelelor, de direcţionarea rapoartelor temporare şi luarea deciziilor. Profesioniştii reţelelor noastre asigură misiunile zilnice de comunicare în vreme ce se confruntă cu activităţi maliţioase.

Testăm politica şi procedurile de securitate ale asigurării informaţiilor prin inspectarea activităţilor. În acest sens avem o politică de inspecţii bazate pe misiuni similare cu cele ale siguranţei nucleare şi pregătim operaţiuni în care sunt antrenate abilităţile noastre de supravieţuire – pentru a opera într-un mediu cât mai apropiat de cel real. Inspectorul general al forţelor aeriene se concentrează pe anumite operaţiuni de manageriere a securităţii informaţiilor prin folosirea elementelor de inspecţie specială. Centrul de informaţii cyber-războinâce conduce şi alte proceduri de evaluare precum: Red Teaming, Computer Security Engineering Assessments, Mulţi Disciplinary Vulnerability Assessments şi Information Assurance Assessment and Assistance Program Assessments. Prin Red Teaming se probează în mod regulat reţelele noastre, rafinând scanările efectuate de CERT şi facilităţile de control ale reţelelor. Suntem verificaţi în mod obiectiv prin Agenţia de Audit a Forţelor Aeriene şi prin controalele inspectorului general.

— Punem în aplicare şi testăm în permanenţă reţelele pentru a ne asigura că informaţiile despre utilizatori sunt disponibile la momentul potrivit şi în formatul potrivit. Scenariile unor posibile evenimente sunt create pentru a permite oamenilor să-şi desfăşoare activitatea folosind procesele şi instrumentele noastre într-un mediu realist. Am participat de curând la simularea CJCS POZITIVE FORCE 2001, care a inclus cel mai mare exerciţiu de apărare a reţelelor – printre jucători numărându-se aproape toate centrele de informaţii, toate serviciile şi

multe agenţii.

— Mai mult, exerciţii anuale precum Joint User Interoperability Communications (JUICE) ne permit să testăm configuraţiile comunicaţiilor portabile şi interfeţele lor, comparându-le cu grila mondială de informaţii. Pe lângă oferirea unor oportunităţi extra ordinare de instruire, astfel de evenimente ne permit să îmbunătăţim configuraţiile echipamentelor, să monitorizăm aplicabilitatea seturilor de instrumente şi să evaluăm procedurile de raportare.

— În plus, forţele aeriene trimit mai multe echipe de suport Scope Network către bazele aeriene pentru a le regla reţelele. Aceste echipe extrem de bine pregătite şi cu obiective clare vor mari performanţa reţelelor din bazele forţelor aeriene prin vizitarea fiecărei instalaţii recente. Prin abordarea lor se va asigura standardizarea, configurarea securităţii şi asigurarea unui nivel standard de performanţă a reţelelor forţelor aeriene. Scope Network vizează optimizarea şi reglarea reţelelor pentru a se asigura că sunt configurate corect. De asemenea, aceste echipe oferă măsuri la îndemână, analize, instruire şi supraveghere pentru a păstra securitatea la cote înalte. Experţii în securitatea informaţiilor însoţesc aceste două funcţii cu detectarea şi direcţionarea eficienţei bunurilor informaţionale.

Ne confruntăm cu o provocare demnă de luat în seamă, la lei ca şi companiile, în legătură cu oamenii ce trebuie recrutaţi, instruiţi şi ni păstrarea tehnicienilor de reţele bine pregătiţi, capabili să construi, im. i, să conducă şi să susţină tehnologiile informaţionale care ne asigură eficienţa. Deşi nu există soluţii simple şi rapide pentru această provocare de personal, continuăm să operăm la un nivel înalt de pregătire. Să vă dau câteva exemple:

— Aşa cum operatorii de avioane şi cei care le întreţin trebuie să fie certificaţi înainte să poată lucra, operatorii de reţele şi cei care le întreţin trebuie să fie

calificaţi înainte de a opera. A fost creată o listă de sarcini esenţiale ale unei misiuni pentru a asigura verificarea calificărilor oricui va coordona o „misiune” de reţea, în acest fel fiind siguri că numai cei care sunt pregătiţi pentru sarcina respectivă sunt aruncaţi în joc. Astfel este îmbunătăţit suportul nostru pentru operaţiunile de luptă. Când sunt chemaţi, aceşti profesionişti licenţiaţi se angajează în războiul informaţional, fiind formată o echipă integrată de operaţiuni informaţionale care să includă un centru mobil de securitate al operaţiunilor de reţea.

— Recunoaştem nu numai că instruirea este foarte importantă pentru oamenii de la securitatea informaţiilor, dar, de asemenea, trebuie să găsim moduri de a-i motiva să rămână în cadrul serviciului. Un studiu al Gartner Group a stabilit că decizia lor de a rămâne este influenţată atât de compensaţiile financiare, cât şi de cele psihologice. Compensaţiile financiare pentru militari constau în bonusuri de reînrolare selectivă pentru 17 din cele 21 de domenii listate (inclusiv cel mai mare bonus disponibil pentru trei domenii de activitate critice). Conducerea forţelor aeriene caută să introducă un bonus pentru abilităţi esenţiale şi un plan de economii pe măsura fondurilor alocate în acest sens. Pentru civili, s-a implementat o bază de salarii speciale pentru lucrătorii de la tehnologia informaţională. Compensaţia psihologică constă într-o serie de iniţiative care ţintesc instruirea, dezvoltarea profesională şi încurajarea iniţiativelor personale. Acestea includ accesul ofiţerilor la sistemele de comunicaţii aerospaţiale, expertiza informaţiei şi dezvoltarea strategiilor. Programul de operaţionalizare şi profesionalizare a reţelelor (OPTN) include continuarea educaţiei ofiţerilor, Centrul de Excelenţă a Forţelor Aeriene Keesler investind în pregătirea tehnică pentru comunicaţiile de bază şi avansate, cursuri suplimentare, centre de pregătire şi instruire profesională, iniţiativa de dezvoltare civilă SCOPE şi serviciul de autoinstruire

disponibil pe portalul forţelor aeriene.

Aceste eforturi se concentrează pe ceea ce facem pentru a îmbunătăţi punctele forte ale oamenilor noştri. De asemenea, trebuie să acordăm atenţie temperării ameninţărilor externe la adresa reţelelor noastre. Hackerii individuali sau grupurile de hackeri s-au înmulţit în ultimul an şi trebuie să rămânem în permanenţă vigilenţi, aşteptându-ne la astfel de atacuri în fiecare zi. Reţelele bune, procedurile bune, instruirea bună şi instrumentele pentru o bună protecţie sunt temelia apărării noastre.

Aşa cum am spus şi mai devreme, viruşii rămân o ameninţare posibilă. În trecutul apropiat, e-mailurile infectate cu viruşii „I Love You” şi „Melissa” au fost deschise de mulţi oameni, ceea ce a făcut ca un număr semnificativ din serverele noastre de e-mail să fie izolate de reţea fie pentru a preveni răspândirea viruşilor, fie pentru a curăţa sistemele afectate. Astăzi, ca urmare a instruirii, recunoaşterii, politicii şi procedurilor, e-mailurile infectate cu viruşi precum „Naked Wife” şi „Anna Kournikova” nu mai sunt deschise. Utilizatorii sistemelor computerizate au primit e-mailuri suspecte şi au luat măsuri potrivite, cum nu au mai fost luate înainte. Cu toate acestea, aceste exemple nu ne lasă să uităm că niciodată NU TREBUIE să lăsăm garda jos.

Daţi-mi voie să subliniez ce facem sau am făcut pentru a lupta împotriva ameninţărilor care vizează sistemele noastre informaţionale:

— Blocarea reţelelor;

— Izolarea punctelor vulnerabile cunoscute;

— Standardizarea protecţiei de bază a informaţiilor şi configurarea sistemelor de firewall;

— Instalarea de software antivirus şi modificarea tuturor unităţilor la apariţia unui nou virus;

— Folosirea sistemelor de detectare a intruziunilor;

— Standardizarea instrumentelor de scanare a

internetului;

— Consolidarea reţelelor şi construirea a noua centre pentru operaţiuni şi securitate.

De asemenea, am dezvoltat şi am folosit o suita de instrumente de apărare pentru centrele de control al reţelelor şi centrele pentru operaţiuni şi securitate.

Următorii paşi

Am realizat foarte multe lucruri de-a lungul ultimilor ani, dar trebuie să continuăm să ridicăm nivelul. Aşa cum congresul a identificat nevoia pentru un sistem de securitate informaţional mai puternic prin aprobarea reformei guvernamentale de securitate a informaţiilor din cadrul documentului de autorizaţie pentru apărare FY2001, forţele aeriene caută şi vor fi în căutarea unei mai bune securităţi. Câteva iniţiative-cheie sunt evidenţiate în cele ce urmează:

— Tehnologia/arhitectura. Forţele aeriene continuă să actualizeze componentele tehnologici informaţionale în toate locaţiile de operare. Sistemul pentru transportul informaţiilor de luptă (CITS), Sistemul de management al reţelelor şi Programul pentru protecţia informaţiilor de bază sunt incluse în cea de a treia etapă, aşa cum am afirmat la începutul prezentei declaraţii. În primele două etape, forţele aeriene au furnizat hardware-ul necesar pentru protejarea barierelor reţelelor, incluzând sisteme de firewall, de detectare a intruziunilor, sisteme de management standardizat al reţelelor în activitate şi din bazele în rezervă şi reţele private virtuale pentru unităţile separate din punct de vedere geografic. Etapa a treia oferă seturi de instrumente pentru managementul şi protejarea intereselor forţelor aeriene prin operaţiunile Comandamentului Major, prin centre de securitate la care se adaugă Centrul de Operaţiuni al Forţelor Aeriene.

— Pe lângă folosirea acestor seturi de instrumente, creăm un intra net al forţelor aeriene pentru a ne limita

expunerea pe internet. Reducem numărul conexiunilor externe de la 109 la 9 centre de operaţiuni şi de securitate a reţelelor. În plus, înfiinţăm o reţea virtuală privată pentru utilizatorii obişnuiţi pentru apărarea şi securizarea întregului trafic de pe site-urile forţelor aeriene.

De asemenea, înfiinţăm reţele virtuale private pentru protejarea anumitor utilizatori.

— Am evaluat concepte precum Info Tech cu lideri din industria IT care acum sunt pe cale să implementeze activitatea forţelor aeriene ca parte a Reţelei Mondiale Informaţionale. Ne îndepărtăm de sistemul de informaţii independente care asigurau buna funcţionare a comunităţilor individuale şi ne îndreptăm spre operaţiuni „centrate pe reţele”, care folosesc aplicaţii web ce susţin utilizatori multipli.

Public Key Infrastructure (PKI) est o altă tehnologie pe care o implementăm în strategia de apărare avansată. Este vorba de utilizarea unei infrastructuri comune, integrate şi interoperabile DoD Public Key pentru a activa serviciile de securitate pe mai multe niveluri.

Common Access Cârd. Adoptăm tehnologia cârdurilor inteligente în cadrul forţelor aeriene. Acestea vor înlocui cârdurile de identificare standard pentru armată, civili şi contractori eligibili. Acest card inteligent va fi folosit pentru a permite accesul fizic în clădiri şi spaţii controlate, dar şi pentru obţinerea accesului la capacităţile reţelei ce calculatoare a departamentului.

Biometrica. Mulţumită bugetului alocat de congres, forţele aeriene au putut implementa elemente ale biometricii pentru a susţine eforturile DoD. Strategia noastră este să folosim noi tehnologii pentru a susţine standardul securităţii informaţiilor împreună cu protecţia contingentelor militare, pregătirea medicală, siguranţa nucleară şi protejarea sistemelor de arme. Am făcut un parteneriat oficial cu Biroul de Management Biometric al Armatei şi Centrul de Fuziune Biometrică. Dezvoltăm

propriul program-pilot în cadrul Agenţiei de Comunicaţii a Forţelor Aeriene. Viitorii paşi ai modernizării criptografice. Forţele aeriene susţin Agenţia pentru Siguranţa Naţională şi efortul OSD de a moderniza capacităţile criptografice. Lucrând împreună cu departamentele operaţionale şi de achiziţii pentru identificarea celor mai urgente nevoi pe care le avem.

Directiva deciziei prezidenţiale 63 (Protejarea infrastructurii). Forţele aeriene merg la unison cu guvernul şi eforturile DoD de a proteja infrastructura esenţială. Avem reprezentanţi pentru fiecare sector de bază ce dezvoltă propriile planuri pentru asigurarea apărării infrastructurii sectorului. În plus, lucrăm cu DoD şi căutăm moduri de a îmbunătăţi procesele funcţionale în desfăşurare, ţintind către o abordare integrată a vulnerabilităţii.

Iniţiative de conducere şi organizaţionale:

Information Operations General Officer Steering Group (IO GOGS). În martie 2000, un grup de conducere al forţelor aeriene a revăzut modul în care organizăm, instruim, echipăm şi susţinem forţele operaţionale informaţionale; s-au oferit îndrumare şi sprijin pentru a asigura integrarea reuşită a investiţiilor semnificative pe care le-am făcut şi avem de gând să le facem. Următorul IO GOGS este programat pentru iunie 2001. La acea întâlnire se vor dezbate numeroase probleme, printre care descrierea informaţiilor tactice, operaţionale şi strategice, protecţia reţelelor, apărarea structurilor şi finalizarea punctelor 2 – 5 din cadrul Doctrinei Forţelor Aeriene.

Grupul de control ai asigurării informaţiilor. Forţele aeriene au stabilit de asemenea un grup transfuncţional de control al asigurării informaţiilor pentru a revizui, dezvolta, coordona şi recomanda poziţiile Asigurării Informaţiilor (AI). Grupul de control este format din ofiţeri cu experienţă şi civili-cheie din forţele aeriene. Reprezentanţi de la cercetare şi dezvoltare, achiziţii,

politică şi comunităţi operaţionale se întâlnesc pentru a revizui strategia, politica, structurile, tehnologia, programele şi condiţiile de finanţare asociate ale Sistemelor de securizare a informaţiilor din cadrul forţelor aeriene. Intenţia grupului de control este să ofere o politică limpede şi logică, să coordoneze eforturile organizaţionale pentru a se asigura că forţele aeriene au resurse pentru implementarea strategiei AI. Information Operations Numbered Air Force (IO NAF). Pe 1 februarie 2001, forţele aeriene au realiniat forţele noastre de război informaţional sub comanda şi structura de control a NAF. Agenţia noastră aeriană de informaţii secrete (care era anterior o agenţie ce opera pe teren subordonată Comandamentului Central al Forţelor Aeriene, reprezentantul personalului pentru operaţiuni) a fost realiniata sub comanda Comandamentului de luptă al 8-lea ce coordona comanda şi capacităţile de control ale forţelor aeriene pentru Asigurarea Informaţiilor şi Operaţiunile Informaţionale.

Operaţiunile de reţele ale forţelor aeriene şi centrul de securitate (AFNOSC). Forţele Aeriene dezvoltă un set de operaţiuni pentru integrarea deplină a securităţii reţelelor şi a funcţiilor operaţiunilor sub un singur comandant ce deţine controlul strategic pentru direcţionarea acţiunilor la nivel înalt. Această capacitate unificată ar trebui să aibă ca rezultat o imagine integrată, operaţional comună, cu un răspuns rapid, o capacitate mare şi un nivel înalt de eficienţă pentru continuarea operaţiunilor. AFNOSC va fi „vârful de lance” pentru tot managementul reţelei forţelor aeriene, asigurarea informaţiei şi apărarea reţelelor de calculatoare.

— Biroul Electronic pentru comunicaţii militare (MCEB). Comunicaţiile între servicii şi agenţii sunt esenţiale pentru succesul luptătorilor angrenaţi în război. Luăm parte la activităţile funcţionale ale MCEB. Funcţiile incluse sunt C41 şi interoperabilitatea sistemelor de date,

managementul frecvenţelor lor, AI, procedurile şi publicările comunicaţiilor militare, operaţiunile de reţele şi testarea interoperabilităţii. MCEB coordonează îndrumarea operaţională şi direcţionarea către CINE, servicii şi agenţii.

Forţele aeriene se concentrează asupra problemelor arzătoare şi asupra construirii programelor care pot oferi cel mai bun serviciu de informaţii şi protejare a informaţiilor posibil. Declararea poziţiei forţelor aeriene subliniază importanţa superiorităţii informaţiilor şi a securităţii informaţiilor, iar programele noastre demonstrează dedicarea cu care luptăm pentru atingerea acestui obiectiv. Avem nevoie de susţinere la toate palierele de securitate informaţională şi în programele infostructurilor de bază. Expunerea tehnologiei noastre informaţionale va susţine efortul forţelor aeriene pentru echilibrarea sistemelor de informaţii care ne garantează superioritatea informaţiilor. Securitatea informaţiilor este cea mai mare prioritate a mea, iar forţele aeriene o pot asigura, dar tot este loc de mai bine. Suntem gata să punem la bătaie orice resurse adiţionale, fie că este vorba despre finanţarea unor capacităţi suplimentare ale sistemului de transport al informaţiilor de luptă, de accelerarea implementării infostructurii de bază, de securizarea tuturor conexiunilor la internet – inclusiv a comutatoarelor telefonice, sau de instruirea şi fidelizarea personalului pe viitor.

Trebuie să explorăm noi căi pentru a investiga şi condamna cu succes atacurile informatice şi infracţiunile pe computer. Temelia legilor tehnologiei noastre informaţionale îşi datorează moştenirea legii telecomunicaţiilor şi anumitor legături cu Legea comunicaţiilor din 1934. A fost una bună şi potrivită la vremea ei. Totuşi, lumea cibernetică se mişcă cu viteza luminii şi avem nevoie de legi în conformitate cu realitatea de azi. Abilitatea de a-i căuta şi prinde pe hackerii care

atacă pagini web sau grupurile organizate de hackeri care pătrund în sistemele de informaţii şi extrag informaţii delicate NU TREBUIE să depindă de procesele penale sau civile ale infractorilor, depăşite de timp. Legea trebuie să fie la curent cu realităţile infracţiunilor cibernetice şi nevoile investigaţionale printr-o „gândire liberă”, precum folosirea cererilor verbale de căutare şi a magistraţilor specializaţi şi instruiţi în domeniul IT. Am înţeles că Departamentul de Justiţie ia în calcul ca legislaţia să reglementeze aceste probleme şi orice astfel de efort merită întreaga noastră atenţie. De asemenea, trebuie să trimitem publicului un mesaj clar şi puternic: „Dacă încălcaţi legile reţelelor de calculatoare, vă vom căuta şi vă vom trage la răspundere”.

Aşa cum am spus mai devreme, toate oportunităţile de beneficii suplimentare pentru războinicii noştri comunicaţionali şi informaţionali – capitalul nostru intelectual – sunt binevenite şi încurajate. Le vom folosi, de exemplu, pentru perfecţionarea abilităţilor-cheie şi ale ofiţerilor comunicaţionali şi pentru continuarea studiilor celor înrolaţi.

Naţiunea noastră şi forţele aeriene pot fi foarte mândre de războinicii noştri comunicaţionali şi informaţionali. În ceea ce priveşte capacitatea de a răspunde în faţa unor potenţiale conflicte şi competenţa superiorităţii informaţionale şi a capacităţii decizionale, armata SUA nu are pereche. Forţele aeriene americane au o mentalitate de învingător, pregătite şi dedicate susţinerii nevoilor de securitate ale naţiunii, oriunde, oricând.

CENTRUL NAŢIONAL PENTRU PROTECŢIA INFRASTRUCTURII (NIPC)

Pentru cei cărora le place să atace internetul, una dintre marile realizări este incapacitatea guvernului de a-i descoperi. În cazul de faţă este vorba despre încetineala cu care FBI a devenit conştient de realitatea unui cyber-

război şi de căutarea unor metode de ai face faţă. Eforturile lor s-au concretizat în înfiinţarea unei organizaţii numite NIPC. NIPC a fost înfiinţat la începutul anului 1998. Mai jos este declaraţia făcută de Michael A. Vatis, directorul NIPC, în faţa congresului, la scurt timp după înfiinţare:

„Daţi-mi voie să explic pe scurt de ce NIPC funcţionează în cadrul FBI. în primul rând, după cum ştiţi, FBI are programe şi a primit autorizaţie pentru a investiga infracţiunile pe computer şi pentru a preveni şi investiga actele de spionaj şi terorism. Aceste programe şi autorizaţii susţin şi fac parte din misiunile de protecţie a infrastructurii. În al doilea rând, în cazul celor mai multe atacuri cibernetice, nu sunt cunoscute nici identitatea, nici obiectivul infractorului. Acest lucru înseamnă că de multe ori este imposibil să stabileşti la început dacă intruziunea este o infracţiune, terorism, activitate străina secretă sau o formă de atac strategic. Singurul mod în care poţi stabili sursa, natura şi scopul incidentului este investigaţia. Competenţa de a investiga astfel de chestiuni – şi de a obţine ordinele judecătoreşti necesare sau citaţiile – cade în seama celor împuterniciţi de lege. Asta nu înseamnă că, odată ce infractorul este identificat şi scopul atacului este cunoscut, reacţiile se limitează doar la aplicarea legii.

Pur şi simplu, înseamnă că, în cazurile în care singurele informaţii pe care le avem sunt că a avut loc o intruziune, dar nu ştim răspunsul la „cine, ce, de ce, sau cum?”, reacţia iniţială trebuie să vină în mod normal din partea organelor statului. Dar în mod sigur FBI trebuie să coopereze şi să aibă susţinerea altor agenţii care pot furniza informaţii relevante. De exemplu, dacă se află că o intruziune este parte a unui atac militar strategic, în mod sigur Departamentul Apărării şi alte agenţii responsabile pentru securitatea naţională ar putea fi solicitate să participe.

Misiune şi structură

NIPC încorporează şi extinde misiunea şi personalul CITAC din cadrul FBI. Misiunea NIPC este să detecteze, să determine, să avertizeze, să răspundă sau să investigheze acte ilegale ce privesc intruziunile informatice şi acte ilegale atât fizice, cât şi cibernetice care ameninţă sau ţintesc infrastructurile noastre de bază. Asta nu înseamnă că investigăm sau răspundem pur şi simplu la atacuri după ce acestea se petrec, ci că încercăm să le anticipăm pentru a le putea preveni. Este o sarcină importantă şi grea. Necesită adunarea şi analizarea informaţiilor culese din toate sursele disponibile (inclusiv investigaţiile permise de lege, surse secrete, date furnizate de companii şi surse publice) şi diseminarea analizelor şi avertizărilor în privinţa unui atac către posibilele victime, fie că sunt din aparatul de stat sau din sectorul privat.

Pentru a îndeplini această misiune, NIPC se bazează pe asistenţa şi informaţiile adunate de cele 57 de birouri FBI din teritoriu, de alte agenţii federale, de stat şi agenţii locale împuternicite prin lege şi, poate cel mai important, sectorul privat.

Departamentul Apărării este important pentru misiunea noastră pentru că dependenţa de informaţii şi tehnologii îl face să fie o primă ţintă pentru adversar şi pentru că deţine o mare parte din resursele guvernamentale de apărare împotriva atacurilor cibernetice. Agenţiile noastre de informaţii secrete au un rol fundamental din cauza responsabilităţii pentru adunarea informaţiilor despre ameninţări venite din afara graniţelor. Alte agenţii civile cu responsabilitate de protecţie care intră sub incidenţa procedurii PDD-63 pentru infrastructurile critice, precum Finanţele, Energia şi Transporturile, au roluri asemănătoare.

Dar protejarea infrastructurii nu este doar o misiune pentru guvernul federal. Guvernele naţionale trebuie să fie implicate pentru că deţin şi operează unele dintre infrastructurile esenţiale şi pentru că agenţiile sunt de

multe ori primele care răspund în cazul unei crize.

În cele din urmă, această misiune necesită implicarea profundă a sectorului privat. Companiile private deţin şi operează cea mai mare parte din infrastructură, aşa că trebuie să fie implicat în eforturile noastre de a le apăra. De asemenea, au cea mai mare putere de expertiză în identificarea şi rezolvarea problemelor tehnice.

Ca recunoaştere a rolurilor vitale pe care aceste entităţi le au, vreau să subliniez că NIPC se bazează pe noţiunea de parteneriat. Construim acest parteneriat în primul rând prin reprezentare generală. Intenţia noastră este ca la centru să fie convocaţi numeroşi profesionişti de la alte agenţii federale, de la companii locale sau de stat şi din sectorul privat. Astfel va fi încurajat schimbul de informaţii şi expertiză şi va fi îmbunătăţită coordonarea dintre toţi cei implicaţi în cazul unei situaţii de criză. În plus, Centrul va spori prezenţa fizică a acestor reprezentanţi prin stabilirea unei conexiuni electronice între numeroasele entităţi diferite din guvern şi sectorul privat care s-ar putea să aibă – sau au nevoie de – informaţii despre ameninţări la adresa infrastructurilor noastre.

La fel de importantă este nevoia de a construi un drum cu două sensuri pentru fluxul de informaţii şi date despre incidente între guvern şi sectorul privat. Guvernul, fiind singurul care are acces la informaţiile secrete naţionale şi la alte informaţii pentru care este împuternicit prin lege, poate avea o imagine de ansamblu asupra ameninţărilor la adresa statului pe care nicio entitate din sectorul privat nu ar putea-o avea pe cont propriu. Trebuie să împărtăşim companiilor cunoştinţele noastre. În acelaşi timp, trebuie să aflăm de la ele informaţii despre încercările de intruziune şi vulnerabilităţile pe care le experimentează. Acest lucru ne va ajuta să ne facem o imagine mai clară despre vulnerabilităţi şi ameninţări şi ne va oferi un punct de pornire pentru prevenirea sau

contracararea unui viitor atac. Este un concept nou pentru noi toţi şi în mod special pentru agenţiile care merg foarte departe pentru a proteja sursele sau metodele folosite. Dar cred că acest dialog este singurul mod de a veni în întâmpinarea preocupării noastre comune pentru protejarea infrastructurii. Credem că este posibilă împărtăşirea informaţiilor necesare despre ameninţări şi vulnerabilităţi fără a pune în pericol sursele sau metodele şi fără a compromite datele din proprietatea companiei. În prezent creăm reguli şi mecanisme pentru a îndeplini acest lucru.

Să vă spun câte ceva şi despre ceea ce nu suntem. Nu suntem un superadministrator de sistem al naţiunii şi nici ofiţerul de securitate responsabil pentru infrastructurile sau sistemele tuturor împotriva impostorilor; nici nu dăm sfaturi despre cel mai nou software de securitate şi nu oferim remedii pentru a rezolva vulnerabilităţile. Acest rol trebuie în mod clar îndeplinit de administratorii de sistem din fiecare companie, de ofiţerii de informaţii din agenţiile guvernamentale şi de grupuri de companii sau alte entităţi (precum echipele de intervenţie în caz de urgenţe) cu expertiză în reducerea vulnerabilităţilor şi restabilirea funcţionării normale a sistemelor. Mai degrabă, rolul nostru este să ajutăm la prevenirea intruziunilor şi atacurilor prin adunarea de informaţii despre ameninţări din surse care sunt disponibile numai guvernului (precum informaţiile secrete), şi combinarea lor cu informaţii furnizate voluntar de sectorul privat sau obţinute din surse publice, prin analize iniţiate şi diseminarea analizelor noastre şi a avertizărilor către toţi utilizatorii interesaţi. Şi, dacă un atac are loc, rolul nostru este să fim punctul central al guvernului federal pentru răspuns la criză şi investigaţii. Aceasta este misiunea centrului. Este o sarcină importantă şi destul de dificilă şi asupra acestui lucru trebuie să ne concentrăm.

Cum este organizat NIPC

Pentru a-şi îndeplini obiectivele, NIPC este organizat în trei secţiuni:

— Secţia de investigaţii şi operaţiuni computerizate (CIOS) este ramura operaţională şi de intervenţie din cadru! NIPC. Prin intermediul ei sunt dirijate investigaţiile atacurilor informatice conduse de birourile teritoriale ale FBI din toată ţara şi se pun la dispoziţia investigatorilor federali sau publici şi a agenţiilor locale guvernamentale implicate în securitatea infrastructurii experţi în domeniu, echipament şi suport logistic.

— Secţia de analiză şi avertizare (AWS) serveşte drept ramură a NIPC pentru sesizări şi avertizări, oferind suport analitic pe parcursul investigaţiilor de atacuri informatice şi analize pe termen lung asupra vulnerabilităţilor şi ameninţărilor. Atunci când este cazul, AWS face avertizări strategice şi trimite analize tuturor partenerilor implicaţi în asigurarea securităţii informaţionale, informându-i în legătură cu posibilele vulnerabilităţi, ameninţări şi tendinţe pe termen lung. De asemenea, AWS analizează zilnic numeroase baze de date guvernamentale sau din sectorul privat, din presă ori din alte surse, pentru a strânge informaţii relevante pentru îndeplinirea misiunii noastre – incluzând aici centralizarea datelor despre atacuri potenţiale.

— Training, Administration and Outreach Section (TAOS) coordonează instruirea şi educarea investigatorilor cibernetici din birourile teritoriale FBI, agenţii locale sau de stat împuternicite de lege şi organizaţii din sectorul privat. Coordonează de asemenea modul în care ajungem la companiile din sectorul privat, conducerile locale sau centrale, alte agenţii guvernamentale şi birourile teritoriale FBI. în plus, această secţiune se ocupă de adunarea şi catalogarea informaţiilor ce au legătură cu „bunurile cheie” din ţară. În cele din urmă, oferă suport administrativ întregului centru, ocupându-se de

problemele legate de personal, buget, contractori şi echipament.

Un document NIPC a oferit mai multe detalii despre teoria conform căreia multe alte agenţii guvernamentale au văzut centrul nostru ca fiind o instituţie ambiţioasă şi nimic mai mult.

NIPC va include persoane din FBI, USSS şi alţi investigatori experimentaţi în infracţiunile pe computer şi protecţia infrastructurii, dar şi reprezentanţi trimişi de Departamentul Apărării, sau provenind din comunitatea informaţiilor secrete şi agenţii de conducere. Centrul va fi conectat electronic la reţelele guvernului federal, inclusiv la cele ale altor centre de avertizare şi operaţiuni, cât şi orice centre de analiză din sectorul privat. Misiunea lui va include avertizarea la timp în cazul ameninţărilor serioase, oferirea unor analize cuprinzătoare, răspunsuri, investigaţii.

Toate departamentele executive şi agenţiile vor coopera cu NIPC şi vor oferi asistenţă, informaţii şi sfaturi pe care NIPC le solicită în limita legii. De asemenea, toate departamentele executive vor împărtăşi NIPC-ului informaţii despre ameninţări, avertizări şi atacuri efective asupra guvernului şi infrastructurilor din sectorul privat, în limita legii. NIPC va include personal responsabil de avertizare, analize, investigaţii computerizate, coordonarea răspunsului în caz de urgenţă, instruire, acţiune şi de folosirea instrumentelor tehnice. În plus, va stabili propriile relaţii directe cu ceilalţi din sectorul privat şi va împărtăşi informaţii cu structurile echivalente din sectorul privat, precum Centrul de Informaţii şi Analize descris în continuare.

NIPC, alături de agenţia de informaţii, va tria informaţiile permise de lege şi de cele secrete pentru includerea lor în analizele şi rapoartele pe care le va oferi, într-o formă adecvată, agenţiilor federale, de stat sau celor locale, celor care operează cu infrastructura esenţială şi

oricărei alte entităţi din sectorul privat de astfel de informaţii şi analize, înainte de diseminarea unor informaţii ce ţin de securitatea naţională şi a altor informaţii provenite de la comunitatea de informaţii secrete, NIPC va coopera în întregime cu întreaga comunitate de informaţii secrete prin procedurile existente. Fie că are rapoarte complete sau nu, NIPC va emite avertizări sau alerte de atac în condiţii de creştere a ameninţării către orice entitate din sectorul privat care împărtăşeşte informaţii şi analize şi către proprietari şi operatori. Aceste avertizări ar putea de asemenea include îndrumare privind luarea de măsuri de protecţie suplimentara de către proprietari şi operatori. Cu excepţia situaţiilor de urgenţă extremă, NIPC va coopera cu centrul naţional de coordonare înainte de emiterea avertizărilor publice pentru atacuri iminente din partea teroriştilor internaţionali, statelor străine sau altor puteri străine ostile.

NIPC va oferi un punct central naţional pentru adunarea de informaţii legate de ameninţări la adresa infrastructurilor. În plus, NIPC va oferi mijloacele principale de facilitare şi coordonare a răspunsului guvernului federal în faţa incidentelor, temperarea atacurilor, investigarea ameninţărilor şi monitorizarea eforturilor de recuperare a sistemelor afectate. În funcţie de nivelul şi natura unei ameninţări sau a unui atac, protocoalele stabilite între agenţiile cu funcţii speciale (DOI/DOD/CIA) şi decizia finală a preşedintelui, NIPC poate primi un rol direct de susţinere fie pentru DOD, fie pentru comunitatea de informaţii secrete.

Centrul de Informaţii şi Analize (ISAC) este coordonatorul naţional, lucrând cu toţi coordonatorii de sector, oficialii de legătură din teritoriu şi Consiliul Economic Naţional. ISAC se va consulta cu proprietarii şi operatorii infrastructurilor esenţiale pentru a încuraja crearea unui centru în sectorul privat pentru împărtăşirea

informaţiilor şi analize. Designul şi funcţiile centrului, precum şi relaţia lui cu NIPC vor fi stabilite de sectorul privat împreună cu şi sub supravegherea guvernului federal. În 180 de zile de la această directivă, coordonatorul naţional, sub supravegherea CICG, incluzând Consiliul Economic Naţional, va identifica metode posibile de a oferi asistenţă federală pentru înlesnirea înfiinţării unui centru de tip ISAC.

Un astfel de centru poate servi ca mecanism pentru colectare, analiză, triere şi diseminare a informaţiilor din sectorul privat atât pentru companii, cât şi pentru NIPC. De asemenea, centrul ar putea aduna, analiza şi disemina informaţii de la NIPC pentru o distribuire viitoare către sistemul privat. Deşi este crucial pentru un parteneriat de succes între guvern şi companii, acest mecanism pentru împărtăşirea informaţiilor importante despre vulnerabilităţi, ameninţări, intruziuni şi anomalii nu trebuie să se amestece în schimburile directe de informaţii dintre companii şi guvern. Cum în final este creat de reprezentanţii sectorului privat, ISAC poate imita anumite aspecte ale unor instituţii precum centrele pentru controlul şi prevenţia bolilor care s-au dovedit foarte eficiente, mai ales în ceea ce priveşte schimburile de amploare între sectoarele private.

Cu un asemenea model, ISAC ar deţine un grad înalt de concentrare tehnică şi expertiză. Ar stabili statistici de bază şi tipare ale diverselor infrastructuri, ar deveni un birou de selectare pentru informaţiile din diferitele sectoare şi ar oferi o arhivă pentru informaţiile mai vechi care să fie folosite de sectorul privat aşa cum va crede de cuviinţă ISAC sau guvernul. Esenţiale pentru succesul unei asemenea instituţii ar fi promptitudinea în răspuns ei, accesibilitatea, coordonarea, flexibilitatea, utilitatea şi acceptabilitatea

GLOSAR

Termeni tehnici utilizaţi în această carte:

Adresa IP – „Internet Protocol Address”, adică ceea ce fiecare computer conectat la internet trebuie să aibă pentru a putea comunica instant cu altul. Gândeşte-te la ea ca şi cum ar fi „numărul de telefon” al internetului.

Adulmecătorii sunt instrumente de hacking care colectează informaţiile ce intră sau ies dintr-un computer (de obicei un server). Informaţia este apoi trimisă către cel care a implantat adulmecătorul. Adulmecătorii sunt utili pentru colectarea parolelor sau a ID-urilor utilizatorilor.

Apache este un program software (cunoscut şi sub numele „software server”) *Open Source Movement* (adică gratis), pentru rularea paginilor web pe un computer-gazdă. Majoritatea site-urilor web pe care le poţi vedea funcţionează cu Apache.

Aparatura wireless pentru internet. La început arătau ca nişte telefoane mobile un pic mai mari, dar erau ataşate la internet în locul sistemului telefonic.

ARPANET vine de la Advanced Research Projects Agency Network. Aşa era numit internetul în anii ’70 şi 80, când încă mai era un proiect de cercetare al Departamentului Apărării.

ASN [National Security Agency (Agenţia pentru Siguranţa Naţională din SUA)] – Este o organizaţie secretă (în timpul Războiului Rece, guvernul nici măcar nu recunoştea că există) care dezvoltă coduri secrete (criptare) pentru a păstra secrete comunicaţiile americane confidenţiale. ASN se ocupă de asemenea şi cu dezlegarea codurilor inamicilor (decriptare). Utilizarea tot mai mare a criptării pe internet a atras o mare parte din atenţia ASN.

Atacul DDOS (Distributed Denial of Service Attack) foloseşte mai multe calculatoare pentru a trimite cantităţi

mari de date către un site. Site-urile pot face faţă doar unui număr limitat de utilizatori conectaţi simultan. În mod normal, aceasta nu este o problemă, dar dacă acaparezi în mod intenţionat toată capacitatea unui site, ca într-un atac DDOS, nimeni altcineva nu mai poate folosi acel site.

Baudul este unitatea de date transferate pe secundă printr-o linie telefonică prin intermediul unui modem. Cu aproximaţie, opt bauzi corespund unei litere sau unei cifre. Aşadar, un modem de 300 de bauzi (din anii ’70) poate transfera aproximativ 37 de caractere pe secundă. Cele mai multe modemuri din ziua de azi operează cu 56.000 de bauzi.

Baza de date este un fişier de pe calculator, de multe ori unul foarte mare, care conţine liste de informaţii (nume, adresă şi alte lucruri pentru toţi clienţii, sau angajaţii, sau orice altceva). Utilizatorii de baze de date folosesc un software special pentru a putea să găsească informaţii în baza de date şi pentru a face actualizări.

Bombe inteligente – vechile bombe obişnuite (învelişuri de metal umplute cu explozibili şi aruncate din avion), cu dispozitive de ghidare ataşate. Acestea conţin mici aripioare alimentate de baterii şi comandate cu ajutorul unui sistem de ghidare. Bombele obişnuite nu sunt foarte exacte, putând ateriza chiar şi la o distanţa de o sută de metri de ţintă. Bombele inteligente au o eroare de până la zece metri.

Buffer Overflow Exploitation este o tehnică prin care trimiţi un anumit tip de date către un server web şi declanşezi manifestarea unei deficienţe a software-ului (comună multor produse Microsoft), lucru care îţi permite să strecori un virus sau un program zombie şi astfel să pătrunzi în server, în ciuda apărării. Există o mulţime de alte tipuri de defecte care pot fi exploatate în acest fel. Atunci când ele sunt descoperite, producătorul software-ului tinde să furnizeze rapid o rezolvare. Dar uneori durează mai mult şi, între timp, se produc pagube. O

temere majoră în rândul cyber-războinicilor este că inamicul va fi primul care va găsi o astfel de deficienţă şi va ţine acest lucru secret. Dacă nu se mai împiedică nimeni altcineva de acesta, cei care ştiu de existenţa sa deţin materialul pentru o cyber-armă puternică.

Bulletin Board System (BBS) este un program pentru computer care permite utilizatorilor să se conecteze la BBS prin modem (în prezent, acest lucru se face prin internet), precum şi să citească şi să scrie mesaje către toate persoanele care utilizează BBS. Versiunea de internet a BBS este Usenet, care are mii de forumuri distincte (pentru subiecte diferite).

Caii troieni sunt programe deghizate în programe legale. Cineva poate modifica un program care, de exemplu, îţi spune în ce zi a săptămânii a căzut o dată oarecare în ultimele două sute de ani. Modificarea adaugă o funcţie care poate face ceva interesant sau ceva periculos. Înainte de apariţia internetului, caii troieni erau o formă enervantă de vandalism de care trebuia să te fereşti. Existau mai multe variaţii, dar ideea de bază din spatele lor era să capeţi pe PC un program de care nu ştiai sau pe care nu îl doreai. La început, caii troieni au fost folosiţi în scop de farse şi realizau doar nişte glume inofensive (de exemplu, nişte gândaci ce mişunau pe ecran). Dar pe parcursul anilor ’80, aceştia au devenit periculoşi; unii dintre ei distrugeau date sau programe. Alţii, odată rulaţi, se răspândeau prin modificarea altui software cu ajutorul propriilor rutine. Cam în aceeaşi perioadă, creatorii de cai troieni au început să transmită rapid software-urile lor infestate prin sistemele BBS. Înainte de asta, cei mai mulţi oameni nu erau online; astfel, cea mai mare parte a software-urilor era transmisă prin dischete. Odată ce BBS-ul a devenit popular, distribuţia a fost mai rapidă, iar caii troieni au ajuns pe (noile) unităţi de hard disk. Din toate acestea s-a născut industria de software antivirus. Şi totuşi, cei mai mulţi

utilizatori de PC nu se complică folosind programe antivirus.

CERT – Computer Emergency Response Te-am, fondată iniţial de Departamentul Apărării SUA în 1988 pentru a analiza rapid înşelătoriile sau dezastrele majore de pe internet. CERT operează în afara Universităţii Carnegie Mellon şi încă mai este principala instituţie internaţională pentru rezolvarea problemelor de pe internet

CIC – Combat Information Center2. Inventat în timpul celui de-al Doilea Război Mondial, când au apărut o mulţime de senzori electronici (radar, aparate de sunet) şi părea o idee bună să trimiţi toate aceste informaţii către o încăpere mare (de pe o navă sau un buncăr) unde aveau să fie sortate, puse pe hărţi şi ecrane pentru a putea fi asimilate de comandanţii care luau deciziile. În ziua de azi, CIC-urile sunt camere pline de monitoare de calculator. La un moment dat, CIC a devenit o sursă pentru descrierile science-fiction despre cum ar trebui să arate „puntea unei nave spaţiale”.

Computerele mainframe sunt cele mai mari, mai scumpe, mai complexe şi mai puternice calculatoare. Acestea, de obicei, acoperă cele mai multe dintre nevoile de caicul pentru o organizaţie mare. Reţine că primele mainframe-uri ale anilor ’60 au mai puţin de unu la sută din viteza şi capacitatea de stocare a celui mai ieftin PC de azi (de 500 $).

Crackerii sunt hackeri puşi pe rele. Aceşti vandali ai internetului mai sunt numiţi şi hackeri black hat. Asta pentru a-i diferenţia de hackerii buni, care sunt cunoscuţi sub numele de hackeri white hat. Practic, internetul a fost construit de o mulţime de hackeri (programatori care analizează o problemă a software-ului până o rezolvă. Aceasta se numeşte „analiză bună”).

Criptarea se referă la utilizarea codurilor pentru a face ca e-mailul sau datele tale să fie dificil (sau imposibil)

de folosit. Criptarea există de mii de ani şi încă mai foloseşte acelaşi principiu de bază al substituirii celor scrise de tine cu alte litere sau cifre. Oricine are cheia decriptării (care arată ce trebuie înlocuit în materialul codat pentru a-l transforma din nou în ceva ce poate fi înţeles) poate citi materialul codat. Computerele au schimbat metoda criptării. Unul dintre primele computere moderne a fost inventat în cel de-al Doilea Război Mondial pentru a decripta codurile germanilor. Încă de pe atunci computerele au fost folosite pentru criptarea şi decriptarea (prin folosirea cheii) mesajelor codate. Teoretic, este posibil să foloseşti un computer pentru a decripta un mesaj codat fără să utilizezi cheia. Dar pentru asta este nevoie de mult timp. În funcţie de cât de puternic este codul criptat, o astfel de „decriptare forţată" este, la urma urmei, din motive practice, imposibilă.

CRT este Cathode Ray Tube. Adică monitorul computerului. În televiziune sunt folosite tipuri diferite de CRT-uri.

Cyber-războinicul este orice specialist militar sau din guvern în domeniul internetului, care ştie cum să atace utilizând reţelele de comunicaţii (cum ar fi internetul) şi să apere reţelele de astfel de atacuri, începând cu al Doilea Război Mondial, acest tip de activitate a fost numit război electronic. Când este implicat internetul, de multe ori sunt cooptaţi şi voluntari civili pentru a duce acest război.

Decriptarea înseamnă spargerea codurilor (chei de criptare) folosite pentru a păstra informaţiile secrete. Înaintea secolului XX, se referea la descifrarea puzzle-urilor, întrucât pe vremea aceea criptarea se baza pe lucruri precum substituirea (folosirea anumitor numere sau simboluri în locul literelor). Dar în ultima sută de ani, au fost create aparate care să utilizeze coduri mai complexe, iar în timpul celui de-al Doilea Război Mondial au fost create computere care să testeze mai rapid toate „substituirile" posibile pentru spargerea codurilor. Practic,

decriptarea se referă fie la folosirea unor computere mai puternice pentru a încerca toate combinaţiile posibile până poţi citi codul, fie la (şi asta îi sperie cel mai mult pe utilizatorii de criptare) folosirea unor algoritmi speciali pentru a găsi erori în rutina de substituire.

Exploatarea datelor se referă la o nouă tehnologie în care sunt folosite cantităţi imense de date, precum achiziţionarea de produse de către milioane de indivizi anual, ca instrument statistic de găsire a unor corelaţii utile. De exemplu, ce fel de produse cumpără oamenii înaintea sau în timpul anumitor evenimente (plecarea în vacanţă, în preajma sărbătorilor) pentru diferite niveluri de venit. Exploatarea datelor dezvăluie tipare de cumpărături necunoscute înainte şi favorizează o mai bună comercializare. Această abordare există de mai bine de un secol, dar, folosind exploatarea datelor beneficiul este mult mai rapid şi mai exact.

Fibra optică este un tip de cablu pentru transferul datelor pe distanţe lungi. Spre deosebire de vechiul cablu (de cupru) care transfera datele prin semnale electrice, fibrele optice folosesc lumina pentru transport prin aceste bucle de cablu. Astfel pot fi transferate mult mai multe date la un preţ mai mic.

FTP, prescurtare de la File Transfer Protocol, este un program de computer care permite utilizatorilor de internet să obţină fişiere (date sau programe) de la un alt computer.

Hackingul îţi foloseşte abilităţile tehnice pentru a lucra la un program sau pe internet. De obicei, intenţia este de a îmbunătăţi modul în care funcţionează software-ul, dar hackerii răi nu urmăresc decât să provoace pagube cât mai mari.

Honey Pot – este un server instalat pe internet şi are unicul scop de a atrage hackeri. Odată ce aceştia găsesc serverul, ceea ce se întâmplă la câteva ore de la pornirea lui, detectorii de intruziune şi instrumentele de

identificare, cu care este echipat Honey Pot, înregistrează tot ce fac hackerii atunci când încearcă să pătrundă. Astfel, hackerii *white hat (*tipii buni) află ce pun la cale hackerii *black hat* (tipii răi). Există o reţea numită Honey Net, între serverele căreia se face schimb de informaţii despre hackeri, informaţii ce sunt comunicate şi agenţiilor de securitate. Majoritatea acestor servere sunt conduse de voluntari care de multe ori suportă din propriul buzunar cheltuielile pentru întreţinerea lor.

Instrument pentru ghicirea parolei – este un program (numit de multe ori şi „dicţionar de parole") care foloseşte o listă extinsă (uneori cu peste un milion de elemente) a parolelor cunoscute sau tipice pentru a putea intra ilegal pe un site sau pe un server protejat prin parolă. Nu ai nevoie decât de un nume de utilizator. Aceste instrumente nu mai sunt la fel de utile cum erau, pentru că tot mai multe site-uri blochează numele de utilizator pentru care se introduc prea multe parole incorecte (între trei şi zece, de exemplu) una după alta. Apoi site-ul îi spune utilizatorului să încerce din nou peste aproximativ cinci minute. Este în regulă pentru un utilizator adevărat şi suficient de mult pentru a face programul de ghicire a parolei ineficient. În acest fel, ar dura zile întregi să testezi sute de mii de parole posibile. Fără acea suspendare, instrumentul de ghicire ar da rezultate în câteva minute sau în cel mult o oră.

ISP înseamnă Internet Service Provider. Acestea sunt companii, precum AOL sau Earthlink, care furnizează utilizatorilor accesul la internet. De fapt, ISP-urile plătesc sume mari de bani companiilor de telefonie care construiesc şi întreţin „coloana vertebrală" a internetului pentru linii de mare capacitate, pe distanţe lungi, ce transportă cea mai mare parte a traficului pe internet (e-mail, cereri de pagini web, descărcarea fişierelor, înţelegi ce vreau să spun).

LAN, prescurtare de la Local Area Network, este un

sistem necostisitor de software şi cabluri care interconectează mai multe PC-uri într-un birou. LAN-ul în sine este de multe ori conectat la internet, astfel încât toţi utilizatorii LAN pot naviga pe **net.**

Linux este un sistem de operare gratuit creat de programatorii *Open Source Movement.* Linux câştigă tot mai multă popularitate printre companii şi instituţii şcolare. Deşi nu este la fel de uşor de instalat şi întreţinut precum produsele comerciale (Microsoft Windows), software-ul este gratuit.

Magnetul minţilor sclipitoare – orice organizaţie sau activitate care atrage mulţi oameni cu bune abilităţi de operare pe computer şi internet. Corporaţia Microsoft este un astfel de magnet, la fel cum sunt şi unele tipuri de software (precum sistemele de operare Linux).

NIPC este Naţional Infrastructure Protection Center. A fost înfiinţat de către FBI pentru a supraveghea prinderea infractorilor pe internet.

NIPRNET este o structură a Departamentului Apărării care are numai câteva conexiuni la internetul obişnuit.

Nodurile sunt unul (sau mai multe) servere (a se vedea definiţia de mai sus) care stochează informaţiile necesare pentru un site.

OPSEC – termenul militar pentru operaţiunile de securitate. Aceasta este denumirea pentru acţiunile pe care le întreprinzi pentru a împiedica duşmanul să intre în serverele bazelor, clădirilor sau de internet.

PAO – este prescurtarea de la Public Affairs Officer. Aceştia sunt cei care au de-a face cu mass-media. Fiecare forţă militară are angajaţi astfel de ofiţeri, întrucât mass-media a devenit o armă tot mai puternică.

Perioada de luare a deciziei este timpul de care ai nevoie ca să recunoşti informaţiile, să **îţi** dai seama la ce se referă, să iei o decizie şi să o pui în practică. În termeni

militari, pilotul sau comandantul unităţii de infanterie care are cea mai scurtă perioadă de luare a deciziei va câştiga. Aceste perioade joacă de asemenea un rol în crearea software-urilor şi combaterea infracţiunilor pe internet. Viteza contează.

Poliţia cibernetică – oameni ai legii (plus un număr de profesionişti ai internetului care îşi oferă ajutorul voluntar) care iau urma infractorilor ce operează pe internet. În anii ’90, cei mai mulţi dintre aceştia învăţaseră tainele meseriei pe cont propriu (poliţişti pentru care computerul era un hobby), dar acum există un mare avânt de a-i instrui pe mulţi dintre oamenii legii astfel încât să poată face faţă infracţiunilor pe internet.

Psyops – este prescurtarea de la operaţiuni psihologice. Jocul cu mintea inamicului. Cea mai simplă formă este lansarea unor fluturaşi deasupra trupelor inamice care explică de ce ar trebui să se predea. În formele mai sofisticate, sunt înfiinţate staţii radio pe care duşmanii le cred de partea lor, dar acestea transmit informaţii demoralizatoare.

Red Attack (sau Echipa Red ori Echipa Tiger) constă într-un grup de experţi în internet care îţi va sparge sistemul pentru a vedea cât de bună este apărarea pe care o ai. Acest lucru poate fi costisitor (începe de la 5.000 $ şi ajunge rapid la şase cifre), în funcţie de cât de mare este sistemul.

Remailer – cunoscut şi sub numele de serviciu remailer anonim. Acesta este un site care ascunde orice informaţie despre e-mailul tău. Trimiţi e-mailul către remailer şi el îţi trimite o adresă anonimă. În unele cazuri, remailerul păstrează informaţii care, în cazul unui ordin judecătoresc, dezvăluie identitatea acelora care folosesc serviciul. Alte remailere distrug orice dovadă a adevăratei identităţi a utilizatorilor. Poliţia şi agenţiile antiteroriste nu agreează astfel de servicii, dar ele pot fi înfiinţate oriunde şi ar fi foarte dificil să fie înlăturate cu totul.

Script Kiddies sunt în general tineri, de multe ori adolescenţi care-şi fac de cap pe internet prin utilizarea instrumentelor de hacking uşor disponibile. Aceştia sunt mai mult o pacoste decât o ameninţare, dar plecând de **aici,** unii trec la hacking serios, ajungând la infracţiuni.

Server – un computer pe care sunt stocate site-urile web. Un server este adesea doar un PC ca acela pe care îl folosim acasă, cu un software special şi o conexiune foarte rapidă la internet. Practic, orice PC poate fi transformat într-un server cu software-ul potrivit şi o conexiune directă la internet (care este destul de scumpă).

SIPRNET este o structură secretă a Departamentului Apărării care trimite toate informaţiile folosind criptarea (codarea) şi nu este conectată la internetul pe care noi ceilalţi îl folosim.

Software **de securitate** – programe care scad şansele computerului tău de a fi avariat de atacurile de pe internet (viruşi, în mod special). Cel mai comun software de securitate este software-ul antivirus (care monitorizează PC-ul cu privire la prezenţa viruşilor şi îi elimină pe cei găsiţi) şi software-ul firewall (care blochează accesul oricărui element dăunător în PC).

Sysadmin este prescurtarea de la System Administrator – administrator de reţea. Acesta este persoana responsabilă de funcţionarea unui site, a unei reţele locale (Local Area Network – LAN) sau a serverului. Nu este o muncă uşoară, întrucât există o mulţime de lucruri care pot merge prost, iar software-ul cu ajutorul căruia funcţionează serverul, site-ul sau reţeaua locală trebuie să fie mereu actualizat pentru a funcţiona în continuare şi a-l proteja de intruşi. Nu sunt niciodată suficient de mulţi administratori de reţea bine pregătiţi şi acest lucru face ca o mulţime de site-uri să fie foarte vulnerabile la atacurile hackerilor.

TCP/IP este setul de standarde al oricărui computer pentru a comunica pe internet. Orice computer cu

software care a aderat la standardele TCP/IP poate fi conectat la internet. Aceasta a fost o idee radicală la vremea respectivă (anii ’70), dar era nevoie de ea pentru a deveni accesibil la scară mare.

Vampirii sunt viermi sau viruşi al căror unic scop este să pătrundă atât de adânc în sistem, încât calculatorul infestat să nu mai poată face nimic altceva. Rezultatul este similar cu ceea ce se întâmplă atunci când ai deschis prea multe programe în acelaşi timp pe PC; lucrează foarte anevoios. Un vampir care rulează pe un server web garantează că cei mai mulţi dintre cei care încearcă să intre pe diverse site-uri de pe acel server vor renunţa, pentru că acesta a încetinit serverul prea mult.

Viermii sunt viruşi care se ataşează de alte programe. De exemplu, Logic Bomb. Acesta este un program ascuns din sistemul computerului care devine activ numai când sunt îndeplinite anumite condiţii. În acel moment, Logic Bomb se declanşează şi face ceva. De obicei, ceva foarte rău. Acest tip de program este inserat, de obicei, de un programator care are acces legal la calculatorul în cauză. Managerii se tem întotdeauna ca nu cumva un programator nefericit (şi concediat de curând) să lase un Logic Bomb care să se declanşeze atunci când el nu mai este prin preajmă pentru a ţine virusul în aşteptare. Atunci când totuşi se declanşează, cauzează lucruri neplăcute, precum ştergerea evidenţei statelor de plată, sau produce daune mai subtile în evidenţa afacerilor.

Cei care creează programe Logic Bomb sunt de obicei prinşi, iar în ultimii ani, tot mai mulţi dintre aceşti flăcăi îndărătnici au fost trimişi la închisoare.

Virusul este un program pentru calculator care, odată infiltrat în computerul tău, va încerca să se răspândească şi în altele prin lista ta de adrese de e-mail şi va face alte lucruri neplăcute computerului tău. În funcţie de fiecare virus (până în 2001 au fost identificaţi 70.000), acesta poate să nu prezinte niciun pericol sau să îţi

distrugă toate datele de pe hard drive.

Zombie este un program cu ajutorul căruia hackerii infectează computerele slab protejate (server ce administrează un site sau un PC cu conexiune la un modem de cablu sau DSL). Există zeci de programe zombie diferite, dar ceea ce au în comun este abilitatea de a comunica cu hackerii pentru a prelua, într-o anumită măsură, controlul asupra computerului pe care l-au infectat. Programele antivirus pot detecta şi elimina programele zombie.